

SELMER RANKS OF QUADRATIC TWISTS OF ELLIPTIC CURVES WITH PARTIAL RATIONAL TWO-TORSION

ZEV KLAGSBRUN

ABSTRACT. This paper investigates which integers can appear as 2-Selmer ranks within the quadratic twist family of an elliptic curve E defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$. We show that if E does not have a cyclic 4-isogeny defined over $K(E[2])$, then subject only to constant 2-Selmer parity, each non-negative integer appears infinitely often as the 2-Selmer rank of a quadratic twist of E . If E has a cyclic 4-isogeny defined over $K(E[2])$ but not over K , then we prove the same result for 2-Selmer ranks greater than or equal to r_2 , the number of complex places of K . We also obtain results about the minimum number of twists of E with rank 0, and subject to standard conjectures, the number of twists with rank 1, provided E does not have a cyclic 4-isogeny defined over K .

1. INTRODUCTION

This paper investigates the integers occurring as 2-Selmer ranks within the quadratic twist family of a given elliptic curve E . Letting $\text{Sel}_2(E/K)$ denote the 2-Selmer group of E (see Section 2 for the definition), we define the 2-Selmer rank of E/K , denoted $d_2(E/K)$, by

$$d_2(E/K) = \dim_{\mathbb{F}_2} \text{Sel}_2(E/K) - \dim_{\mathbb{F}_2} E(K)[2].$$

Definition 1.1. For $X \in \mathbb{R}^+$, define a set

$$S(X) = \{\text{Quadratic } F/K : \mathbf{N}_{K/\mathbb{Q}} \mathfrak{f}(F/K) < X\}$$

where $\mathfrak{f}(F/K)$ is the finite part of the conductor of F/K . For each $r \in \mathbb{Z}^{\geq 0}$ define a quantity $N_r(E, X)$ by

$$N_r(E, X) = |\{F/K \in S(X) : d_2(E^F/K) = r\}|,$$

where E^F is the quadratic twist of E by F/K .

The 2-Selmer rank of E serves as an upper bound for the Mordell-Weil rank of E so understanding its distribution within quadratic twist families helps us understand the rank distribution within the

This paper is based on work conducted by the author as part of his doctoral thesis at UC-Irvine under the direction of Karl Rubin and was supported in part by NSF grants DMS-0457481 and DMS-0757807. The author would like to express his utmost gratitude to Karl Rubin for the guidance and assistance he provided while undertaking this research.

twist family. We are therefore concerned with the limiting behavior of $\frac{N_r(E, X)}{|S(X)|}$ as $X \rightarrow \infty$. Recent work by Kane, building on work of Swinnerton-Dyer and Heath-Brown showed that if E is defined over \mathbb{Q} , $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and E does not have a cyclic 4-isogeny defined over \mathbb{Q} , then $\frac{N_r(E, X)}{|S(X)|}$ tends to an explicit non-zero limit α_r for every non-negative integer r such that sum of the α_r over $r \in \mathbb{Z}^{\geq 0}$ is equal to 1 [Kan10], [SD08], [HB94]. Additional recent work by this author, Mazur, and Rubin proves that if $E(K)[2] = 0$ and $\text{Gal}(K(E[2])/K) \simeq \mathcal{S}_3$, then a similar result holds using a different method of counting after correcting by some local factors arising over totally complex fields [KMR11].

Far less is known about the behavior $\frac{N_r(E, X)}{|S(X)|}$ for curves with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and this paper provides a partial answer. Most notably we prove the following:

Theorem 1.1. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over $K(E[2])$. Then $N_r(E, X) \gg \frac{X}{\log X}$ for all non-negative $r \equiv d_2(E/K) \pmod{2}$. If E does not have constant 2-Selmer parity, then $N_r(E, X) \gg \frac{X}{\log X}$ for all $r \in \mathbb{Z}^{\geq 0}$.*

This result is similar to earlier results of Mazur and Rubin for curves with $E(K)[2] = 0$.

Constant 2-Selmer parity is a phenomenon exhibited by certain curves E , where $d_2(E^F/K) \equiv d_2(E/K) \pmod{2}$ for all quadratic twists E^F of E . Dokchitser and Dokchitser have shown that E/K has constant 2-Selmer parity if and only if K is totally imaginary and E acquires everywhere good reduction over an abelian extension of K [DD11].

Constant 2-Selmer parity is one of two known obstructions to a non-negative integer r appearing as the 2-Selmer rank of some twist of E . A second obstruction can occur when the condition that E not have a cyclic 4-isogeny defined over $K(E[2])$ is relaxed. This author recently exhibited an infinite family of curves over any number field K with a complex place such that $d_2(E^F/K) \geq r_2$ for every curve E in this family and every quadratic F/K , where r_2 is the number of complex places of K [Kla11]. This lower-bound phenomenon is not well understood, but appears to be independent of constant 2-Selmer parity.

We are however able to prove the following results in the special case where E has a cyclic 4-isogeny defined over $K(E[2])$ but not over K .

Theorem 1.2. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over K . If E has a twist E^F such that $d_2(E^F/K) = r$, then $N_r(E, X) \gg \frac{X}{\log X}$.*

Theorem 1.3. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over K . Then $N_r(E, X) \gg \frac{X}{\log X}$ for all $r \geq r_2$ with $r \equiv d_2(E/K) \pmod{2}$, where r_2 is the number of conjugate pairs of complex embeddings of K . If E does not have constant 2-Selmer parity, then $N_r(E, X) \gg \frac{X}{\log X}$ for all $r \geq r_2$.*

Theorem 1.3 limits the lower-bound obstruction and shows that the curves presented in [Kla11] exhibit the worst possible behavior in regard to lower-bound obstruction among curves that do not have a cyclic 4-isogeny defined over K . The next theorem further limits the lower-bound obstruction, essentially saying that it can't apply to both E and E' simultaneously, where E' is the curve 2-isogenous to E .

Theorem 1.4. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over K .*

- (i) *Then either $N_r(E, X) \gg \frac{X}{\log X}$ for all $r \in \mathbb{Z}^{\geq 0}$ with $r \equiv d_2(E/K) \pmod{2}$ or $N_r(E', X) \gg \frac{X}{\log X}$ for all $r \in \mathbb{Z}^{\geq 0}$ with $r \equiv d_2(E/K) \pmod{2}$.*
- (ii) *If E does not have constant 2-Selmer parity, then we additionally have that either $N_r(E, X) \gg \frac{X}{\log X}$ for all $r \in \mathbb{Z}^{\geq 0}$ with $r \not\equiv d_2(E/K) \pmod{2}$ or $N_r(E', X) \gg \frac{X}{\log X}$ for all $r \in \mathbb{Z}^{\geq 0}$ with $r \not\equiv d_2(E/K) \pmod{2}$.*
- (iii) *If either K has a real place or E has a place of multiplicative reduction, then $N_r(E, X) \gg \frac{X}{\log X}$ for all $r \in \mathbb{Z}^{\geq 0}$ or $N_r(E', X) \gg \frac{X}{\log X}$ for all $r \in \mathbb{Z}^{\geq 0}$. (I.E. The choice of E and E' for parts (i) and (ii) can be taken to be the same.)*

As the 2-Selmer rank of E serves as an upper bound for the rank of E , we are able to prove the following corollaries.

Corollary 1.5. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over K . If either $d_2(E/K) \equiv 0 \pmod{2}$ or E does not have constant 2-Selmer parity, then the number of twists E^F of E having Mordell-Weil rank 0 grows at least as fast as $\frac{X}{\log X}$.*

In order to say something about E having twists of rank one, we need to rely on the following well-known conjecture that is a consequence of the Tate-Shafarevich conjecture.

Conjecture 1.6 (Conjecture III $T_2(K)$). *For every elliptic curve E defined over K , $\dim_{\mathbb{F}_2} \text{III}(E/K)[2]$ is even.*

The 2-Selmer group sits inside the exact sequence

$$0 \rightarrow E(K)/2E(K) \rightarrow \text{Sel}_2(E/K) \rightarrow \text{III}(E/K)[2] \rightarrow 0.$$

As $\dim_{\mathbb{F}_2} E(K)/2E(K) = \text{rank } E/K + \dim_{\mathbb{F}_2} E(K)[2]$, if Conjecture $\text{IIIT}_2(K)$ holds and $d_2(E/K) = 1$, then the Mordell-Weil rank of E will be 1. We can therefore state the following:

Corollary 1.7. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over K . Assuming conjecture $\text{IIIT}_2(K)$ holds and either $d_2(E/K) \equiv 1 \pmod{2}$ or E does not have constant 2-Selmer parity, then the number of twists E^F of E having rank one grows at least as fast as $\frac{X}{\log X}$.*

Other results similar to Corollaries 1.5 and 1.7 when $E(K)[2] = 0$ are due to Ono and Skinner when $K = \mathbb{Q}$ and to Rubin and Mazur for general K . Similar results when $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are due to Skorobogatov and Swinnerton-Dyer [OS98] [MR10], [SSD05].

1.1. Layout. We begin in Section 2 by recalling the definition of the 2-Selmer group and presenting a technique developed by Mazur and Rubin to compare the 2-Selmer group of E with that of E^F . Section 3 develops similar machinery for the Selmer group associated with a 2-isogeny of E . In Section 4 we explore what it means for E to have a cyclic 4-isogeny over K and over $K(E[2])$. We prove Theorem 1.2 in Section 5. Theorem 1.1 is proved Sections 6 and 7. Lastly, in Section 8 we develop techniques specific to curves with cyclic 4-isogenies defined over $K(E[2])$ and use them to prove Theorems 1.3 and 1.4.

The proofs of Lemmas 6.2 and 7.1 are simpler in the case where E does not have a cyclic 4-isogeny defined over $K(E[2])$ than in the case where E acquires a cyclic 4-isogeny over $K(E[2])$. We therefore include the proof for the former case in the main text and relegate the proof for latter case to Appendix A. Some of the results in Section 8 require local calculations specific to curves that acquire a cyclic 4-isogeny over $K(E[2])$ and some of these calculations appear in Appendix B.

2. THE 2-SELMER GROUP

2.1. Background. We begin by recalling the definition of the 2-Selmer group. If E is an elliptic curve defined over a number field K , then $E(K)/2E(K)$ maps into $H^1(K, E[2])$ via the Kummer map. The 2-Selmer group of E is a subgroup of $H^1(K, E[2])$ that attempts to bound the part of $H^1(K, E[2])$ cut out by the image of $E(K)/2E(K)$. We can map $E(K_v)/2E(K_v)$ into $H^1(K_v, E[2])$ via the Kummer map for any completion K_v of K , and the following diagram commutes for every place v of K , where δ is the Kummer map.

$$\begin{array}{ccc} E(K)/2E(K) & \xrightarrow{\delta} & H^1(K, E[2]) \\ \downarrow & & \downarrow \text{Res}_v \\ E(K_v)/2E(K_v) & \xrightarrow{\delta} & H^1(K_v, E[2]) \end{array}$$

For each place v of K , we define a distinguished local subgroup $H_f^1(K_v, E[2]) \subset H^1(K_v, E[2])$ by $\text{Image}(\delta : E(K_v)/2E(K_v) \hookrightarrow H^1(K_v, E[2]))$. We define the **2-Selmer group** of E/K , denoted $\text{Sel}_2(E/K)$, by

$$\text{Sel}_2(E/K) = \ker \left(H^1(K, E[2]) \xrightarrow{\sum \text{res}_v} \bigoplus_{v \text{ of } K} H^1(K_v, E[2]) / H_f^1(K_v, E[2]) \right).$$

That is, the 2-Selmer group is the group of cohomology class in $H^1(K, E[2])$ whose restrictions locally come from points of $E(K_v)$ in each completion K_v of K .

The 2-Selmer group is a finite dimensional \mathbb{F}_2 -vector space that sits inside the exact sequence of \mathbb{F}_2 -vector spaces

$$0 \rightarrow E(K)/2E(K) \rightarrow \text{Sel}_2(E/K) \rightarrow \text{III}(E/K)[2] \rightarrow 0,$$

where $\text{III}(E/K)$ is the Tate-Shafaravich group of E .

Definition 2.1. We define the **2-Selmer rank** of E , denoted $d_2(E/K)$, by

$$d_2(E/K) = \dim_{\mathbb{F}_2} \text{Sel}_2(E/K) - \dim_{\mathbb{F}_2} E(K)[2].$$

One of the ways in which we study the 2-Selmer group of E is by studying the local conditions $H_f^1(K_v, E[2])$. The following lemma provides us with a way to do that.

Lemma 2.2. (i) If $v \nmid 2\infty$, then $\dim_{\mathbb{F}_2} H_f^1(K_v, E[2]) = \dim_{\mathbb{F}_2} E(K_v)[2]$

(ii) If $v \nmid 2\infty$ and E has good reduction at v then

$$H_f^1(K_v, E[2]) \simeq E[2]/(Frob_v - 1)E[2]$$

with the isomorphism given by evaluation of cocycles in $H_f^1(K_v, E[2])$ at the Frobenius automorphism $Frob_v$.

Proof. This is Lemma 2.2 in [MR10]. □

We would like to examine the behavior of $\text{Sel}_2(E/K)$ under the action of twisting by a quadratic extension.

Definition 2.3. Let E be given by $E : y^2 = x^3 + Ax^2 + Bx + C$ and F/K be a quadratic extension given by $F = K(\sqrt{d})$. The **quadratic twist** of E by F denoted E^F is the elliptic curve given by the model $y^2 = x^3 + dAx^2 + d^2Bx + d^3C$.

There is an isomorphism $E \rightarrow E^F$ given by $(x, y) \mapsto (dx, d^{3/2}y)$ defined over F . Restricted to $E[2]$, this map gives a canonical G_K isomorphism $E[2] \rightarrow E^F[2]$. This allows us to view $H_f^1(K_v, E^F[2])$ as sitting inside $H^1(K_v, E[2])$. We will study $\text{Sel}_2(E^F/K)$ by considering the relationship between $H_f^1(K_v, E[2])$ and $H_f^1(K_v, E^F[2])$. This relationship is addressed by the following lemma due to Kramer.

Given a place w of F above a place v of K , we get a norm map $E(F_w) \rightarrow E(K_v)$, the image of which we denote by $E_{\mathbf{N}}(K_v)$.

Lemma 2.4. *Viewing $H_f^1(K_v, E^F[2])$ as sitting inside $H^1(K_v, E[2])$, we have*

$$H_f^1(K_v, E[2]) \cap H_f^1(K_v, E^F[2]) = E_{\mathbf{N}}(K_v)/2E(K_v)$$

Proof. This is Proposition 7 in [Kra81] and Proposition 5.2 in [MR07]. The proof in [MR07] works even at places above 2 and ∞ . \square

This equality gives rise to the following lemma:

Lemma 2.5. *Let E be an elliptic curve defined over K , v a place of K , and F/K be a quadratic extension. Then*

- (i) $H_f^1(K_v, E[2]) = H_f^1(K_v, E^F[2])$ if either v splits in F/K or v is a prime where E has good reduction that is unramified in F/K
- (ii) $H_f^1(K_v, E[2]) \cap H_f^1(K_v, E^F[2]) = 0$ if $v \nmid 2\infty$, E has good reduction at v , and v is ramified in F/K .

Proof. Part (i) is Lemma 2.10 in [MR10] and part (ii) is Lemma 2.11 in [MR10]. \square

Lemma 2.6. *Suppose E has good reduction at a prime v away from 2 and F/K is a quadratic extension ramified at v . Then $E^F(K_v)$ contains no points of order 4. It follows that $H_f^1(K_v, E^F[2])$ is the image of $E^F(K_v)[2]$ under the Kummer map.*

Proof. Since E had good reduction at v , $v \nmid 2$, and F/K is ramified at v , Tate's algorithm gives us that E^F has reduction type I_0^* at v . Since E^F has additive reduction at c , we have an exact sequence

$$0 \rightarrow E_1^F(K_v) \rightarrow E_0^F(K_v) \rightarrow k_v^+ \rightarrow 0,$$

where $E_0^F(K_v)$ is the group of points of non-singular reduction on $E^F(K_v)$, $E_1^F(K_v)$ is isomorphic to the formal group of $E^F(K_v)$, and k_v is the residue field of K at v . Since k_v^+ and $E_1^F(K_v)$ have no points of order 2, we get that $E_0^F(K_v)$ has no points of order 2. Because E^F has reduction type I_0^* at v , $E^F(K_v)/E_0^F(K_v) \subset \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (see Table 4.1 in section IV.9 of [Sil94]). It then follows

that $E^F(K_v)$ has no points of order 4. As $E^F(K_v)$ is given by $E^F(K_v)[2^\infty] \times B$ for some profinite group B of odd order, we get that $H_f^1(K_v, E^F[2]) = E^F(K_v)[2^\infty]/2E^F(K_v)[2^\infty] = E^F(K_v)[2]$. \square

2.2. The Method of Rubin and Mazur. Mazur and Rubin developed a technique to use the comparison between the local conditions for E and E^F to compare the Selmer groups $\text{Sel}_2(E/K)$ and $\text{Sel}_2(E^F/K)$. We explain this technique here.

Let E be an elliptic curve defined over a number field K and T a finite set of places of K . We define a localization map

$$\text{loc}_T : H^1(K, E[2]) \rightarrow \bigoplus_{v \in T} H^1(K_v, E[2])$$

as the sum of the restriction maps over the places v in T . We define the strict and relaxed Selmer group, denoted S_T and S^T respectively, by

$$S_T = \ker \left(\text{loc}_T : \text{Sel}_2(E/K) \rightarrow \bigoplus_{v \in T} H^1(K_v, E[2]) \right)$$

and

$$S^T = \ker \left(\text{loc}_T : H^1(K, E[2]) \rightarrow \bigoplus_{v \notin T} H^1(K_v, E[2]) / H_f^1(K_v, E[2]) \right).$$

Lemma 3.2 in [MR10] shows that $\dim_{\mathbb{F}_2} S^T - \dim_{\mathbb{F}_2} S_T$ is given by

$$\dim_{\mathbb{F}_2} S^T - \dim_{\mathbb{F}_2} S_T = \sum_{v \in T} \dim_{\mathbb{F}_2} H_f^1(K_v, E[2]).$$

The following theorem of Kramer provides an important relationship between the parities of $d_2(E/K)$ and $d_2(E^F/K)$.

Theorem 2.7 (Kramer).

$$d_2(E/K) \equiv d_2(E^F/K) + \sum_{v \text{ of } K} \dim_{\mathbb{F}_2} E(K_v) / E_{\mathbf{N}}(K_v)$$

Proof. This is Theorem 2.7 in [MR10]; also see Remark 2.8 there as well. \square

The following proposition is the main ingredient in the method of Rubin and Mazur. We reproduce it here along with their proof.

Proposition 2.8 (Proposition 3.3 in [MR10]). *Let E be an elliptic curve defined over a number field K . Suppose F/K is a quadratic extension such that all places above $2\Delta_E\infty$ split in F/K , where Δ_E is the discriminant of some model of E . Let T be the set of (finite) primes \mathfrak{p} of K such that F/K is ramified at \mathfrak{p} and $E(K_{\mathfrak{p}})[2] \neq 0$. Set $V_T = \text{loc}_T(\text{Sel}_2(E/K))$. Then*

$$d_2(E^F/K) = d_2(E/K) - \dim_{\mathbb{F}_2} V_T + d$$

for some d satisfying

$$(1) \quad 0 \leq d \leq \dim_{\mathbb{F}_2} \left(\bigoplus_{\mathfrak{p} \in T} H_f^1(K_{\mathfrak{p}}, E[2]) \right) / V_T$$

and

$$(2) \quad d \equiv \dim_{\mathbb{F}_2} \left(\bigoplus_{\mathfrak{p} \in T} H_f^1(K_{\mathfrak{p}}, E[2]) \right) / V_T \pmod{2}.$$

Proof. Let $V_T^F = \text{loc}_T(\text{Sel}_2(E^F/K))$. Lemma 2.5 gives us that $H_f^1(K_v, E^F[2]) = H_f^1(K_v, E[2])$ for all $v \notin T$ and therefore $S_T \subset \text{Sel}_2(E^F/K)$. This gives us that the sequences

$$0 \rightarrow S_T \rightarrow \text{Sel}_2(E/K) \rightarrow V_T \rightarrow 0$$

and

$$0 \rightarrow S_T \rightarrow \text{Sel}_2(E^F/K) \rightarrow V_T^F \rightarrow 0$$

are exact. We therefore get that

$$d_2(E^F/K) = d_2(E/K) - \dim_{\mathbb{F}_2} V_T + \dim_{\mathbb{F}_2} V_T^F.$$

We will let $d = \dim_{\mathbb{F}_2} V_T^F$ and show that it satisfies the conditions above.

Since $H_f^1(K_v, E[2]) \cap H^1(K_v, E^F[2]) = 0$ for all $v \in T$ by part (ii) of Lemma 2.5, we have

$$\begin{aligned} \dim_{\mathbb{F}_2} V_T + \dim_{\mathbb{F}_2} V_T^F &= \dim_{\mathbb{F}_2} \text{Sel}_2(E/K)/S_T + \dim_{\mathbb{F}_2} \text{Sel}_2(E^F/K)/S_T \\ &\leq \dim_{\mathbb{F}_2}(S^T/S_T) = \sum_{v \in T} \dim_{\mathbb{F}_2} H_f^1(K_v, E[2]). \end{aligned}$$

The last equality follows from Lemma 3.2 in [MR10]. This gives us that

$$\dim_{\mathbb{F}_2} V_T^F \leq \sum_{v \in T} \dim_{\mathbb{F}_2} H_f^1(K_v, E[2]) - \dim_{\mathbb{F}_2} V_T = \dim_{\mathbb{F}_2} \left(\bigoplus_{\mathfrak{p} \in T} H_f^1(K_{\mathfrak{p}}, E[2]) \right) / V_T,$$

giving us the first condition above.

To get the parity result, we will apply Theorem 2.7. Observe that Lemma 2.4 and part (i) of Lemma 2.5 tell us that $\dim_{\mathbb{F}_2} E(K_v)/E_{\mathbf{N}}(K_v) = 0$ for all $v \notin T$ and that $\dim_{\mathbb{F}_2} E(K_v)/E_{\mathbf{N}}(K_v) = \dim_{\mathbb{F}_2} H_f^1(K_v, E[2])$ for all $v \in T$. We therefore have that

$$\dim_{\mathbb{F}_2} V_T + \dim_{\mathbb{F}_2} V_T^F \equiv \sum_{v \in T} \dim_{\mathbb{F}_2} H_f^1(K_v, E[2]) \pmod{2}$$

so

$$\dim_{\mathbb{F}_2} V_T^F \equiv \dim_{\mathbb{F}_2} \left(\bigoplus_{\mathfrak{p} \in T} H_f^1(K_{\mathfrak{p}}, E[2]) \right) / V_T \pmod{2}.$$

□

3. THE ϕ -SELMER GROUP

In the setting of Proposition 2.8, if F/K is an extension such that T contains a single prime \mathfrak{p} , then $d_2(E^F/K) - d_2(E/K)$ can often be read off of (1) and (2) by considering the localization of $\text{Sel}_2(E/K)$ at \mathfrak{p} . Mazur and Rubin developed a strategy for curves with $E(K)[2] = 0$ in which one carefully constructs an extension F/K so that $d_2(E^F/K) - d_2(E/K)$ can be read off of Proposition 2.8. This construction breaks down when $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ because the action of G_K on $E[2]$ is no longer irreducible. By utilizing the Selmer group associated to the 2-isogeny of E , we are able to develop a more complicated strategy that allows us to extend their results to the case when $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$.

3.1. Background. If E is an elliptic curve defined over K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, then E can be given by an integral model over $y^2 = x^3 + Ax^2 + Bx$ defined over K . The subgroup $C = E(K)[2]$ is then generated by the point $P = (0, 0)$.

Given this model, we are able to define a degree 2 isogeny $\phi : E \rightarrow E'$ with kernel C , where E' is given by a model $y^2 = x^3 - 2Ax^2 + (A^2 - 4B)x$ and ϕ is given by $\phi(x, y) = \left(\left(\frac{x}{y} \right)^2, \frac{y(B-x^2)}{x^2} \right)$ for $(x, y) \notin C$. If we define $C' = \phi(E[2])$, then we get a short exact sequence of G_K modules

$$0 \rightarrow C \rightarrow E[2] \xrightarrow{\phi} C' \rightarrow 0.$$

This short exact sequence gives rise to a long exact sequence of cohomology groups

$$(3) \quad 0 \rightarrow C \rightarrow E(K)[2] \xrightarrow{\phi} C' \xrightarrow{\delta} H^1(K, C) \rightarrow H^1(K, E[2]) \xrightarrow{\phi} H^1(K, C') \rightarrow \dots$$

The map δ is given by $\delta(Q)(\sigma) = \sigma(R) - R$ where R is any point on E with $\phi(R) = Q$.

In terms of the localization of the 2-Selmer group, we observe that if $c \in \text{Sel}_2(E/K)$ comes from $H^1(K, C)$, then by part (i) of Lemma 2.2, the localization of c at any prime of good reduction will lie in C . We define the ϕ -Selmer group of E , denoted $\text{Sel}_\phi(E/K)$, to capture the part of $\text{Sel}_2(E/K)$ that comes from $H^1(K, C)$. We construct $\text{Sel}_\phi(E/K)$ in a manner similar to the construction of $\text{Sel}_2(E/K)$.

The following diagram commutes for every place v of K .

$$\begin{array}{ccc} E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(K, C) \\ \downarrow & & \downarrow \text{Res}_v \\ E'(K_v)/\phi(E(K_v)) & \xrightarrow{\delta} & H^1(K_v, C) \end{array}$$

We define distinguished local subgroups $H_\phi^1(K_v, C) \subset H^1(K_v, C)$ for each place v of K as the image of $E'(K_v)/\phi(E(K_v))$ under δ for each place v of K and define $\text{Sel}_\phi(E/K)$ as

$$\ker \left(H^1(K, C) \xrightarrow{\oplus_v \text{Res}} \bigoplus_{v \text{ of } K} H^1(K_v, C)/H_\phi^1(K_v, C) \right).$$

The group $\text{Sel}_\phi(E/K)$ is a finite dimensional \mathbb{F}_2 -vector space and we denote its dimension $\dim_{\mathbb{F}_2} \text{Sel}_\phi(E/K)$ by $d_\phi(E/K)$.

By identifying C with μ_2 , we are able to explicitly identify $H^1(K, C)$ with $K^\times/(K^\times)^2$ and $H^1(K_v, C)$ with $K_v^\times/(K_v^\times)^2$ and consider $\text{Sel}_\phi(E/K)$ as a subgroup of $K^\times/(K^\times)^2$. Explicitly, with the models as above, the map $E'(K_v)/\phi(E(K_v))$ is given by $(x, y) \mapsto x(K_v^\times)^2$ for $(x, y) \neq (0, 0)$ and $(0, 0) \mapsto \Delta_E(K_v^\times)^2$.

The local condition $H_\phi^1(K_v, C)$ is given by $H_\phi^1(K_v, C) = H_u^1(K_v, C)$ for all finite places away from 2 where E has good reduction (see Lemma 4.1 in [Cas65]).

The isogeny ϕ on E gives rise to the dual isogeny $\hat{\phi}$ on E' with kernel $C' = \phi(E[2])$. Exchanging the roles of (E, C, ϕ) and $(E', C', \hat{\phi})$ in the above defines the $\hat{\phi}$ -Selmer group of E' , $\text{Sel}_{\hat{\phi}}(E'/K)$, as a subgroup of $H^1(K, C')$. The following theorem allows us to relate the ϕ -Selmer group, the $\hat{\phi}$ -Selmer group, and the 2-Selmer group.

Theorem 3.1. *The ϕ -Selmer group, the $\hat{\phi}$ -Selmer group, and the 2-Selmer group sit inside the exact sequence*

$$(4) \quad 0 \rightarrow E'(K)[2]/\phi(E(K)[2]) \rightarrow \text{Sel}_\phi(E/K) \rightarrow \text{Sel}_2(E/K) \xrightarrow{\phi} \text{Sel}_{\hat{\phi}}(E'/K).$$

Proof. This is a well known diagram chase. See Lemma 2 in [FG08] for example. \square

3.2. Duality Between $H_\phi^1(E/K)$ and $H_{\hat{\phi}}^1(E'/K)$. A second relationship between the ϕ -Selmer group and the $\hat{\phi}$ -Selmer group arises from a duality between their respective local conditions.

Proposition 3.2. *The sequence*

$$(5) \quad 0 \rightarrow C'/\phi(E(K_v)[2]) \rightarrow H_\phi^1(K_v, C) \rightarrow H_f^1(K_v, E[2]) \xrightarrow{\phi} H_{\hat{\phi}}^1(K_v, C') \rightarrow 0$$

sitting inside sequence (3) is exact.

Proof. This is a well-known result. See Remark X.4.7 in [Sil09] for example. \square

Lemma 3.3 (Local Duality). *For each place v of K there is a local Tate pairing $H^1(K_v, C) \times H^1(K_v, C') \rightarrow \{\pm 1\}$ induced by a pairing $[\cdot, \cdot] : C \times C' \rightarrow \{\pm 1\}$ given by $[Q, \tilde{R}] = \langle Q, R \rangle$ where $\langle Q, R \rangle$ is the Weil pairing and R is any pre-image of \tilde{R} under ϕ . The subgroups defining the local conditions $H_\phi^1(K_v, C)$ and $H_{\hat{\phi}}^1(K_v, C')$ are orthogonal complements under this pairing.*

Proof. Orthogonality is equation (7.15) and the immediately preceding comment in [Cas65]. Combining this orthogonality with exact sequence (5) gives that $H_\phi^1(K_v, C)$ and $H_\phi^1(K_v, C')$ are orthogonal complements. \square

Definition 3.4. The ratio

$$\mathcal{T}(E/E') = \frac{|\text{Sel}_\phi(E/K)|}{|\text{Sel}_\phi(E'/K)|}$$

is called the **Tamagawa ratio** of E .

Because of the duality in Lemma 3.3, the Tamagawa ratio can be computed using a local product formula.

Theorem 3.5 (Cassels). *The Tamagawa ratio $\mathcal{T}(E/E')$ is given by*

$$\mathcal{T}(E/E') = \prod_{v \text{ of } K} \frac{|H_\phi^1(K_v, C)|}{2}.$$

Proof. This is a combination of Theorem 1.1 and equations (1.22) and (3.4) in [Cas65]. \square

We further have the following parity condition.

Theorem 3.6 (Dokchitser, Dokchitset).

$$d_2(E/K) \equiv \text{ord}_2 \mathcal{T}(E/E') \pmod{2}.$$

Proof. This is Corollary 5.8 in [DD11]. \square

3.3. Relationship Between $H_\phi^1(K_v, C)$ and $H_\phi^1(K_v, C^F)$. As noted earlier, if F/K is a quadratic extension, then there is a canonical G_K -isomorphism $E[2] \rightarrow E^F[2]$. If C is a subgroup of $E(K)$ of order 2, then we denote the image of C in $E^F(K)[2]$ by C^F . As the map $C^F \rightarrow C$ is G_K invariant, we can view $H_\phi^1(K_v, C^F)$ as a subgroup of $H^1(K_v, C)$ and $\text{Sel}_\phi(E^F/K)$ as a subgroup of $H^1(K, C)$. This can be thought of as identifying both $H^1(K, C)$ and $H^1(K, C^F)$ with $K^\times/(K^\times)^2$ and both $H^1(K_v, C)$ and $H^1(K_v, C^F)$ with $K_v^\times/(K_v^\times)^2$.

The following four lemmas are an analogue of Lemma 2.5 that allow us to compare $H_\phi^1(K_v, C)$ and $H_\phi^1(K_v, C^F)$.

Lemma 3.7. *Suppose v is a prime away from 2 where E has good reduction and v is ramified in F/K . Then $H_\phi^1(K_v, C^F) = E'^F(K_v)[2]/\phi(E^F(K_v)[2])$.*

Proof. Since v is a prime away from 2, $E^F(K_v)$ is given by $E^F(K_v)[2^\infty] \times B$ and $E'^F(K_v)$ is given by $E'^F(K_v)[2^\infty] \times B'$ where B and B' are profinite abelian groups of odd order. Since ϕ has degree 2, we therefore get that $E'^F(K_v)/\phi(E^F(K_v)) = E'^F(K_v)[2^\infty]/\phi(E^F(K_v)[2^\infty])$. By Lemma 2.6, neither $E^F(K_v)$ nor $E'^F(K_v)$ have any points of order 4, yielding the result. \square

Lemma 3.8 (Criteria for equality of local conditions after twist). *If any of the following conditions hold:*

- (i) v splits in F/K
- (ii) v is a prime away from 2 where E has good reduction and v is unramified in F/K
- (iii) v is a prime away from 2 where E has good reduction, v is ramified in F/K , and $E(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z} \simeq E'(K_v)[2]$

then $H_\phi^1(K_v, C) = H_\phi^1(K_v, C^F)$ and $H_\phi^1(K_v, C') = H_\phi^1(K_v, C'^F)$.

Proof.

- (i) In this case $E \simeq E^F$ over K_v .
- (ii) If v is a prime away from 2 where E has good reduction and v is unramified in F/K , then E^F also has good reduction at v . It then follows that both $H_\phi^1(K_v, C^F)$ and $H_\phi^1(K_v, C)$ are equal to $H_u^1(K_v, C)$ and both $H_\phi^1(K_v, C')$ and $H_\phi^1(K_v, C'^F)$ are equal to $H_u^1(K_v, C')$.
- (iii) By Lemma 3.7, $H_\phi^1(K_v, C^F) = E'^F(K_v)[2]/\phi(E^F(K_v)[2])$. Since $E(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z} \simeq E'(K_v)[2]$, we therefore get that $H_\phi^1(K_v, C^F)$ is given by the image of C'^F in $H^1(K_v, C)$. Since the image of C'^F is generated by Δ_E , E has good reduction at v , and $\Delta_E \notin (K_v^\times)^2$, we get that the image of C'^F is $H_u^1(K_v, C)$ and therefore that $H_\phi^1(K_v, C) = H_\phi^1(K_v, C^F)$. Exchanging the roles of E and E' then gives the result. \square

Lemma 3.9. *Suppose E has good reduction at a prime v away from 2 and F/K is a quadratic extension ramified at v . If $E(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $E'(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then both of $H_\phi^1(K_v, C^F)$ and $H_\phi^1(K_v, C'^F)$ have \mathbb{F}_2 dimension 1 and both $H_\phi^1(K_v, C) \cap H_\phi^1(K_v, C^F) = 0$ and $H_\phi^1(K_v, C') \cap H_\phi^1(K_v, C'^F) = 0$. Further, if F_1/K_v and F_2/K_v are different quadratic extensions of K_v both of which are ramified, then $H_\phi^1(K_v, C^{F_1}) \cap H_\phi^1(K_v, C^{F_2}) = 0$.*

Proof. The fact that $H_\phi^1(K_v, C^F)$ and $H_\phi^1(K_v, C'^F)$ both have \mathbb{F}_2 dimension 1 is an immediate consequence Lemma 3.7. Further, as a subgroup of $K_v^\times/(K_v^\times)^2$, $H_\phi^1(K_v, C^F)$ is generated by the image of Q' , where $Q' \in E'^F[2] - C'^F$. If F/K is locally given by $F_w = K_v(\sqrt{\pi})$, then the point Q' on E^{F_w} is given by $(u\pi, 0)$, where $(u, 0) \in E'(K_v)[2]$. Since $H_\phi^1(K_v, C) = H_u^1(K_v, C)$, it follows

that $\text{ord}_v u$ is even. Since $v \nmid 2$ and F_w is ramified at v , we get that $\text{ord}_v \pi$ is odd. Since Q' maps to $u\pi(K_v^\times)^2$, $H_\phi^1(K_v, C^F)$ is a ramified subgroup of $H^1(K_v, C)$ and therefore disjoint from $H_\phi^1(K_v, C) = H_u^1(K_v, C)$. Exchanging the roles of E and E' completes the first part of the result.

Since $F_1 \neq F_2$, we may write $F_1 = K_v(\sqrt{\pi})$ and $F_2 = K_v(\sqrt{w\pi})$, where $w \in O_{K_v}^\times - (O_{K_v}^\times)^2$. By the above, we get that $H_\phi^1(K_v, C^{F_1})$ is generated by $u\pi(K_v^\times)^2$ and $H_\phi^1(K_v, C^{F_2})$ is generated by $uw\pi(K_v^\times)^2$. Since $w \notin (K_v^\times)^2$, the result follows. \square

Lemma 3.10. *Suppose E has good reduction at a prime v away from 2 and F/K is a quadratic extension ramified at v . If $E(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and $E'(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, then $H_\phi^1(K_v, C^F) = 0$ and $H_\phi^1(K_v, C'^F) = H^1(K_v, C)$.*

Proof. This follows immediately from Lemma 3.7. \square

4. CHARACTERIZATION OF CURVES WITH $E(K) \simeq \mathbb{Z}/2\mathbb{Z}$

For the remainder of this paper, we will assume that $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, $M = K(E[2])$, and $M' = K(E'[2])$.

The results obtained in this paper are dependent on whether E has a cyclic isogeny defined over K or over $K(E[2])$. The following result characterizes such curves.

Lemma 4.1. *Let E be an elliptic curve defined over K with $E(K) \simeq \mathbb{Z}/2\mathbb{Z}$.*

- (i) *E has a cyclic 4-isogeny defined over K if and only if $M' = K(E'[2]) = K$.*
- (ii) *E does not have a cyclic 4-isogeny defined over K but acquires a cyclic 4-isogeny over $M = K(E[2])$ if and only if $M = M'$*

Proof. We begin with the following two observations. First, if $R \in E(\overline{K})$ with $2R = P$, then $\phi(R) \in E'[2] - C'$. Second, if $Q' \in E'[2] - C'$ and $R \in E(\overline{K})$ with $\phi(R) = Q'$, then $2R = \hat{\phi}(Q') = P$.

Suppose that E has a cyclic 4-isogeny defined over K . Let $H = \langle R \rangle$ be a cyclic subgroup of order 4 fixed by G_K . Since $2R \in E[2]$ and $2R$ is fixed by G_K , we get that $2R = P$. We will show that $\phi(R) \in E'(K)$. Let $\sigma \in G_K$. As ϕ is defined over K , $\sigma(\phi(R)) = \phi(\sigma(R))$. However, since $\sigma(R) \in R + C$ for all $\sigma \in G_K$, it follows that $\sigma(\phi(R)) = \phi(R)$. Since $\phi(R) \in E'[2] - C$ and $\phi(R)$ is defined over K , we therefore get that $M' = K$.

Now suppose that E does not have a cyclic 4-isogeny defined over K . Let $Q' \in E'[2] - C'$ and take $R \in E(\overline{K})$ with $\phi(R) = Q'$. Since E does not have a cyclic 4-isogeny defined over K , there is some $\sigma \in G_K$ such that $\sigma(R) \notin \langle R \rangle = \{0, R, P, R + P\}$. We therefore have that $\sigma(\phi(R)) = \phi(\sigma(R)) \neq \phi(R)$. Since $\phi(R) \in E'[2] - C'$, it follows that $M' \not\subset K$. This proves (i).

Further, replacing K by M shows that if E does not have a cyclic 4-isogeny defined over M , then $M' \not\subset M$.

Now suppose that E does not have a cyclic 4-isogeny defined over K but acquires a cyclic 4-isogeny over $M = K(E[2])$. That is, there is a point $R \in E(\overline{K})$ of order 4 such that $\langle R \rangle$ is fixed by G_M . If R is a point of order 4 on E such that $2R \neq P$, then $\phi(R)$ is a point of order 4 such that $2\phi(R) \in C'$. Since $M' \not\subset K$, M' being contained in M is equivalent to M being contained in M' . By passing to E' if necessary, we can therefore assume that $2R = P$. We therefore get that $\sigma(R) \in R + C$ for all $\sigma \in G_M$ and that $\phi(\sigma(R)) = \phi(R)$ for all $\sigma \in G_M$. As $\phi(\sigma(R)) = \sigma(\phi(R))$, we get that $\phi(R) \in E'(M)$. Since $\phi(R) \in E'[2] - C'$, this gives $M' \subset M$. As E did not have a cyclic 4-isogeny defined over K , we have $K \subsetneq M' \subset M$, showing that $M = M'$, completing the proof of (ii). \square

The following corollary follows immediately.

Corollary 4.2. *With E as in Lemma 4.1: If E possesses a cyclic 4-isogeny defined over M but not one defined over K , then $\dim_{\mathbb{F}_2} E(K_v)[2] = \dim_{\mathbb{F}_2} E'(K_v)[2]$ for all places v of K .*

5. PROOF OF THEOREM 1.2

For the remainder of this paper, we will be assuming that $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and that E does not have a cyclic 4-isogeny defined over K . For simplicity, we will let $C = E(K)[2]$ be generated by a point P and fix a second point Q of order 2 so that $E[2] = \langle P, Q \rangle$.

The proofs of our main theorems are based on constructing an extension F/K ramified at a small number of places in such a fashion that $d_2(E^F/K) - d_2(E/K)$ may be read off of (1) and (2).

Lemma 5.1. *Define S to be the image of $H^1(K, C)$ in $H^1(K, E[2])$ under the map in (3) and let $V \subseteq H^1(K, E[2])$ be a dimension r subspace of $H^1(K, E[2])$ such that $V \cap S = 0$. Then there exist $\sigma_1, \dots, \sigma_r \in G_K$ such that $\sigma_i|_M \neq 1$ and $\text{loc}(V)$ has dimension r where the localization map $\text{loc} : H^1(K, E[2]) \rightarrow \bigoplus_{i=1}^r E[2]/C$ is defined by $c \mapsto (c(\sigma_1), \dots, c(\sigma_r))$.*

Proof. Let \tilde{Q} be the image of Q in $E[2]/C$. Take $\tilde{V} \subseteq H^1(K, C')$ to be the image of V in $H^1(K, C') = \text{Hom}(G_K, C')$ and observe that \tilde{V} has dimension r since $V \cap \text{Image}(H^1(K, C)) = 0$. Take a basis $\{c_1, \dots, c_r\}$ for \tilde{V} . Since the image of the dual map $G_K \rightarrow \text{Hom}(\tilde{V}, C')$ is surjective and has dimension r as well, we can find $\tau_1, \dots, \tau_r \in G_K$ such that

$$c_i(\tau_j) = \begin{cases} \tilde{Q} & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

Suppose $\tau_i \in G_M$ for all i . Then the map $G_M \rightarrow \text{Hom}(\tilde{V}, C')$ must be surjective as well. So taking any $\tau \in G_K - G_M$, we can therefore find $\gamma_1, \dots, \gamma_r \in G_M$ such that

$$c_i(\gamma_j) = \begin{cases} \tilde{Q} + c_j(\tau) & \text{if } i = j \\ c_j(\tau) & \text{if } i \neq j \end{cases}$$

Thus,

$$c_j(\gamma_i \tau) = c_j(\gamma_i) + c_j(\tau) = \begin{cases} \tilde{Q} & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

Taking $\sigma_i = \gamma_i \tau$ then gives the result.

Otherwise, we have $\tau_k \notin G_M$ for some k . Define $\sigma_1, \dots, \sigma_r$ by

$$\sigma_i = \begin{cases} \tau_i & \text{if } \tau_i \notin G_M \\ \tau_i \tau_k & \text{if } \tau_i \in G_M \end{cases}$$

We then get that

$$c(\sigma_i) = 0 \ \forall i \Leftrightarrow c(\tau_i) = 0 \ \forall i$$

which means that the localization map is injective on V giving us the result. \square

The following proposition is a consequence of Lemma 5.1 that will be used to prove Theorem 1.2.

Proposition 5.2. *Let E be an elliptic curve over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not have a cyclic 4-isogeny defined over K . If $r = d_2(E/K)$, then*

$$N_r(E, X) \gg \frac{X}{\log X}.$$

Proof. Pick $R \in E(\overline{K})$ such that $2R = P$. Since E does not have a cyclic 4-isogeny over K , there exists some $\tau \in G_K$ such that $\tau(R) \notin \langle R \rangle = \{0, R, P, R + P\}$. Letting c_0 be the co-cycle $c_0 : G_K \rightarrow E[2]$ given by $c_0(\sigma) = \sigma(R) - R$ for $\sigma \in G_K$, we see that $c_0(\tau) \notin C$ and therefore that the element of $\text{Sel}_2(E/K)$ coming from P does not come from $H^1(K, C)$. By Lemma 5.1, we may therefore find $\gamma \in G_K$ such that $\gamma|_M \neq 1$ such that $c_0(\gamma)$ is non-trivial in $E[2]/C$.

Let N be a finite Galois extension of K containing $MK(8\Delta_{E\infty})$ such that the restriction of $\text{Sel}_2(E/K)$ to N is zero, where $K(8\Delta_{E\infty})$ is the ray class field modulo $8\Delta_{E\infty}$. Let $\mathfrak{p}_1, \mathfrak{p}_2$ be primes of K where E has good reduction, not dividing 2, where $\text{Frob}_{\mathfrak{p}_1}$ in $\text{Gal}(N/K)$ is the conjugacy class of $\gamma|_N$ and $\text{Frob}_{\mathfrak{p}_2}$ in $\text{Gal}(N/K)$ is the conjugacy class of $\gamma^{-1}|_N$. Since $\gamma\gamma^{-1}|_{K(8\Delta_{E\infty})} = 1$, $\mathfrak{p}_1\mathfrak{p}_2$ has a totally positive generator $\pi \equiv 1 \pmod{8\Delta_E}$. Letting $F = K(\sqrt{\pi})$, we get that all places dividing $2\Delta_{E\infty}$ split in F/K , and $\mathfrak{p}_1, \mathfrak{p}_2$ are the only primes that ramify in F/K .

We then apply Proposition 2.8 with $T = \{\mathfrak{p}_1, \mathfrak{p}_2\}$. Since E has good reduction at \mathfrak{p}_1 and \mathfrak{p}_2 , it follows from Lemma 2.2 that $H_f^1(K_{\mathfrak{p}_1}, E[2]) = E[2]/(\gamma - 1)E[2] = E[2]/C$, $H_f^1(K_{\mathfrak{p}_2}, E[2]) =$

$E[2]/(\gamma^{-1} - 1)E[2] = E[2]/C$ and that the localization $\text{loc}_T : \text{Sel}_2(E/K) \rightarrow H_f^1(K_{\mathfrak{p}_1}, E[2]) \oplus H_f^1(K_{\mathfrak{p}_2}, E[2])$ is given by $c \mapsto (c(\gamma), c(\gamma^{-1}))$.

If $c \in H^1(K, E[2])$, then we have $0 = c(1) = c(\gamma\gamma^{-1}) = c(\gamma) + c(\gamma^{-1})$, giving that $c(\gamma) = -c(\gamma^{-1})$. Letting V_T be the image of $\text{Sel}_2(E/K)$ under the localization map, we therefore get that V_T is contained in the one dimensional diagonal subspace of $H_f^1(K_{\mathfrak{p}_1}, E[2]) \oplus H_f^1(K_{\mathfrak{p}_2}, E[2])$. Since $c_0(\gamma)$ is non-trivial in $E[2]/C$, we get that V_T is in fact equal to the diagonal subspace in $H_f^1(K_{\mathfrak{p}_1}, E[2]) \oplus H_f^1(K_{\mathfrak{p}_2}, E[2])$.

By Proposition 2.8, we then get that $d_2(E^F/K) = d_2(E/K)$.

Next, observe that if we fix \mathfrak{p}_1 , we still have complete liberty in choosing \mathfrak{p}_2 subject to the conditions on its Frobenius. The Chebotarev density theorem then gives the result. \square

Proof of Theorem 1.2. We follow the proof of Theorem 1.4 in [MR10]. Suppose $d_2(E^F/K) = r$. Every twist $(E^F)^{L'}$ of E^F is also a twist E^L of E and

$$\mathfrak{f}(L/K)|\mathfrak{f}(F/K)\mathfrak{f}(L'/K)$$

$$\text{so } N_r(E, X) \geq N_r\left(E^F, \frac{X}{\mathbf{N}_{K/\mathbb{Q}}\mathfrak{f}(F/K)}\right).$$

Since possession of a cyclic 4-isogeny defined over K is fixed under twisting, E^F does not possess a cyclic isogeny of degree 4 defined over K . The result then follows from applying Proposition 5.2 to E^F . \square

6. TWISTING TO DECREASE SELMER RANK

As shown in the proof of Proposition 5.2, Lemma 5.1 allows us to effectively use Lemma 2.8 as long as the image of $\text{Sel}_\phi(E/K)$ in $\text{Sel}_2(E/K)$ is not too large. The following proposition provides another example of this.

Proposition 6.1. *Let E be an elliptic curve defined over a number field K such that $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and E does not have a cyclic 4-isogeny defined over K . If $\dim_{\mathbb{F}_2}\text{Sel}_\phi(E/K) \leq \dim_{\mathbb{F}_2}\text{Sel}_2(E/K) - 2$, then E has a twist E^F such that $d_2(E^F/K) = d_2(E/K) - 2$.*

Proof. Let S be the image of $\text{Sel}_\phi(E/K)$ in $\text{Sel}_2(E/K)$. Since $E'(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ by Lemma 4.1, $\text{Sel}_\phi(E/K)$ maps 2-1 into $\text{Sel}_2(E/K)$ by Theorem 3.1. As $\dim_{\mathbb{F}_2}\text{Sel}_\phi(E/K) \leq \dim_{\mathbb{F}_2}\text{Sel}_2(E/K) - 2$, we can therefore find a 3-dimensional \mathbb{F}_2 -subspace $V \subset \text{Sel}_2(E/K)$ such that $V \cap S = 0$. Pick $\gamma_1, \gamma_2, \gamma_3 \in G_K$ as in Lemma 5.1 and set $\gamma_4 = (\gamma_1\gamma_2\gamma_3)^{-1}$.

Let N be a finite Galois extension of K containing $MK(8\Delta_{E\infty})$ such that the restriction of $\text{Sel}_2(E/K)$ to N is zero. Choose 4 primes $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$, and \mathfrak{p}_4 not dividing 2 such that E has good reduction and each \mathfrak{p}_i and $\text{Frob}_{\mathfrak{p}_i}|_N = \gamma_i|_N$ for $i = 1, \dots, 4$. Since $\gamma_1\gamma_2\gamma_3\gamma_4|_{K(8\Delta_{E\infty})} = 1$, the ideal

$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ has a totally positive generator π with $\pi \equiv 1 \pmod{8\Delta_E\infty}$. Setting $F = K(\sqrt{\pi})$, it follows that all places dividing $2\Delta_E\infty$ split in F/K , and $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$, and \mathfrak{p}_4 are the only primes that ramify in F/K .

We can therefore apply Proposition 2.8 with $T = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4\}$. Since none of $\gamma_1, \gamma_2, \gamma_3$ were trivial on M , it follows that $\gamma_4|_M \neq 1$ as well. Since E has good reduction at each of the \mathfrak{p}_i , it follows from part (ii) of Lemma 2.2 that $H_f^1(K_{\mathfrak{p}_i}, E[2]) = E[2]/(\gamma_i - 1)E[2] = E[2]/C$ and that the localization map

$$\text{loc}_T : \text{Sel}_2(E/K) \rightarrow H_f^1(K_{\mathfrak{p}_1}, E[2]) \oplus H_f^1(K_{\mathfrak{p}_2}, E[2]) \oplus H_f^1(K_{\mathfrak{p}_3}, E[2]) \oplus H_f^1(K_{\mathfrak{p}_4}, E[2])$$

is given by

$$c \mapsto (c(\gamma_1), c(\gamma_2), c(\gamma_3), c(\gamma_4)).$$

Let V_T be the image of $\text{Sel}_2(E/K)$ under the localization map. By choosing γ_1, γ_2 , and γ_3 in accordance with Lemma 5.1, we ensure that V_T has dimension at least 3. If $c \in H^1(K, E[2])$, then $0 = c(1) = c(\gamma_1\gamma_2\gamma_3\gamma_4) = c(\gamma_1) + c(\gamma_2) + c(\gamma_3) + c(\gamma_4)$, showing that $(0, 0, 0, Q) \notin V_T$ and there that V_T has dimension exactly 3. Proposition 2.8 therefore gives that $d_2(E^F/K) = d_2(E/K) - 2$. \square

The key observation to using Proposition 6.1 to obtain twists of E with reduced 2-Selmer rank is realizing that the size of the image of $\text{Sel}_\phi(E/K)$ in $\text{Sel}_2(E/K)$ can be controlled effectively.

Lemma 6.2. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over K . If both $d_\phi(E/K) > 1$ and $d_{\hat{\phi}}(E'/K) > 1$, then E has a quadratic twist E^F such that*

- (a) $d_\phi(E^F/K) < d_\phi(E/K)$,
- (b) $d_2(E^F/K) = d_2(E/K)$ or $d_2(E^F/K) = d_2(E/K) - 2$, and
- (c) $\mathcal{T}(E^F/E'^F) \leq \mathcal{T}(E/E')$

Proof. We will present the proof for the case when E does not have a cyclic 4-isogeny defined over M here and refer to the reader to Appendix A for the proof when E acquires a cyclic 4-isogeny over M . The requirement that $d_{\hat{\phi}}(E'/K) > 1$ is required only in that latter case.

Suppose E does not have a cyclic 4-isogeny defined over M . Pick $R \in E(\overline{K})$ such that $2R = P$. Since E does not have a cyclic 4-isogeny over M , there exists some $\tau \in G_M$ such that $\tau(R) \notin \langle R \rangle = \{0, R, P, R + P\}$. Letting c_0 be the co-cycle $c_0 : G_K \rightarrow E[2]$ given by $c_0(\sigma) = \sigma(R) - R$ for $\sigma \in G_K$, we see that $c_0(\tau) \notin C$. Observing that

$$\phi(c_0(\sigma)) = \phi(\sigma(R) - R) = \phi(\sigma(R)) - \phi(R) = \sigma(\phi(R)) - \phi(R)$$

for $\sigma \in G_K$, we see that $\tau(\phi(R)) \neq \phi(R)$ since $c_0(\tau) \notin C = \ker \phi$. Recalling that $\phi(R) \in E'[2]$ from the proof of Lemma 4.1, this shows that τ does not fix $E'[2]$ and therefore that $\tau|_{M'} \neq 1$.

Since $d_\phi(E/K) > 1$, we can find $b \in \text{Sel}_\phi(E/K)$ such that b does not come from C' . Since b does not come from C' , taking $N_b = \overline{K}^{\text{Ker } b}$, we get that $N_b \neq M$. We may therefore find $\gamma \in G_K$ such that $\gamma|_{MM'} = \tau$ and $\gamma|_{N_b} \neq 1$.

Let N be a finite Galois extension of K containing $MK(8\Delta_E\infty)$ such that the restrictions of $\text{Sel}_2(E/K)$ and $\text{Sel}_\phi(E/K)$ to N are zero. Let \mathfrak{p}_1 and \mathfrak{p}_2 be primes of K away from 2 where E has good reduction such that $\text{Frob}_{\mathfrak{p}_1}$ in $\text{Gal}(N/K)$ is the conjugacy class of $\gamma|_N$ and $\text{Frob}_{\mathfrak{p}_2}$ in $\text{Gal}(N/K)$ is the conjugacy class of $\gamma^{-1}|_N$. Since $\gamma\gamma^{-1}|_{K(8\Delta_E\infty)} = 1$, $\mathfrak{p}_1\mathfrak{p}_2$ has a totally positive generator $\pi \equiv 1 \pmod{8\Delta_E}$. Letting $F = K(\sqrt{\pi})$, we get that all places dividing $2\Delta_E\infty$ split in F/K , and that \mathfrak{p}_1 and \mathfrak{p}_2 are the only primes that ramify in F/K .

We now apply Proposition 2.8 with $T = \{\mathfrak{p}_1, \mathfrak{p}_2\}$. Since E has good reduction at \mathfrak{p}_1 and \mathfrak{p}_2 , it follows that $H_f^1(K_{\mathfrak{p}_1}, E[2]) = E[2]/(\gamma - 1)E[2] = E[2]$, $H_f^1(K_{\mathfrak{p}_2}, E[2]) = E[2]/(\gamma^{-1} - 1)E[2] = E[2]$ and that the localization map $\text{loc}_T : \text{Sel}_2(E/K) \rightarrow H_f^1(K_{\mathfrak{p}_1}, E[2]) \oplus H_f^1(K_{\mathfrak{p}_2}, E[2])$ is given by $c \mapsto (c(\gamma), c(\gamma^{-1}))$. If $c \in H^1(K, E[2])$, then we have $0 = c(1) = c(\gamma\gamma^{-1}) = c(\gamma) + c(\gamma^{-1})$ giving that $c(\gamma) = -c(\gamma^{-1})$. Letting V_T be the image $\text{Sel}_2(E/K)$ under the localization map, we therefore get that V_T is contained in the two-dimensional diagonal subspace of $E[2] \times E[2]$.

As $b \in \text{Sel}_\phi(E/K)$, we may view it as an element of $\text{Sel}_2(E/K)$. Taking any co-cycle \hat{b} representing b , we get that $\hat{b}(\gamma) \neq 0$ since $\gamma|_{N_b} \neq 1$ and that $\hat{b}(\gamma) \in C$ since $b \in H^1(K, C)$. By design, $c_0(\gamma) \notin C$. As c_0 represents the element of $\text{Sel}_2(E/K)$ coming from P , we therefore get that V_T is the entire two-dimensional diagonal subspace of $E[2] \times E[2]$. Proposition 2.8 therefore gives $d_2(E^F/K) = d_2(E/K)$ or $d_2(E^F/K) = d_2(E/K) - 2$.

By Lemma 3.10, $\text{Sel}_\phi(E^F/K) \subset \text{Sel}_\phi(E/K)$. Since \mathfrak{p}_1 was chosen that so that b did not localize trivially at \mathfrak{p}_1 and $H_\phi^1(K_{\mathfrak{p}_1}, C^F) = 0$, we get that $b \notin \text{Sel}_\phi(E^F/K)$ and therefore that $d_\phi(E^F/K) < d_\phi(E/K)$. Lastly, since $H_\phi^1(K_v, C^F) = H_\phi^1(H_v, C)$ for all $v \neq \mathfrak{p}_1, \mathfrak{p}_2$ and $H_\phi^1(K_{\mathfrak{p}_1}, C^F) = H_\phi^1(K_{\mathfrak{p}_2}, C^F) = 0$, we get that $\mathcal{T}(E^F/E'^F) < \mathcal{T}(E/E')$ by Theorem 3.5.

The case where E has a cyclic 4-isogeny defined over $K(E[2])$ is proved in Lemma A.3. \square

We can combine Proposition 6.1 and Lemma 6.2 into the following Proposition.

Proposition 6.3. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over K and let $t = \max\{0, \text{ord}_2 \mathcal{T}(E/E')\}$. If $d_2(E/K) \geq 2 + t$, then E has a twist E^F such that $d_2(E^F/K) = d_2(E/K) - 2$ and $\mathcal{T}(E^F/E'^F) \leq \mathcal{T}(E/E')$. In the special case where $\mathcal{T}(E/E') \leq 1$, E will have a twist E^F such that $d_2(E^F/K) = d_2(E/K) - 2$ and $\mathcal{T}(E^F/E'^F) \leq 1$ whenever $d_2(E/K) \geq 2$.*

Proof. We can iteratively apply Lemma 6.2 until we end up with a twist E^{F_1} of E with either $d_2(E^{F_1}/K) = d_2(E/K) - 2$, $d_\phi(E^{F_1}/K) = 1$, or $d_\phi(E'^{F_1}/K) = 1$. If $d_2(E^{F_1}/K) = d_2(E/K) - 2$, then take $E^F = E^{F_1}$ giving the result. If $d_\phi(E^{F_1}/K) = 1$ and $d_2(E^{F_1}/K) = d_2(E/K)$, then we have $d_2(E^{F_1}/K) \geq 2$ and we can apply Proposition 6.1 to E^{F_1} , letting E^F be the result of doing so.

If $d_\phi(E'^{F_1}/K) = 1$ and $d_2(E^{F_1}/K) = d_2(E/K)$, then $d_\phi(E^{F_1}/K) = 1 + \text{ord}_2 \mathcal{T}(E^{F_1}/E'^{F_1}) \leq 1 + \text{ord}_2 \mathcal{T}(E/E')$. We therefore have

$$d_2(E^{F_1}/K) = d_2(E/K) \geq 2 + \text{ord}_2 \mathcal{T}(E/E') \geq 2 + \text{ord}_2 \mathcal{T}(E^{F_1}/E'^{F_1}) = d_\phi(E^{F_1}/K) + 1$$

and are able to apply Proposition 6.1 to E^{F_1} , letting E^F be the result of doing so. \square

7. TWISTING TO INCREASE SELMER RANK

We are also able to utilize the ϕ -Selmer group to construct a twist E^F of E with $d_2(E^F/K) = d_2(E/K) + 2$.

Lemma 7.1. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over K . Then E has a twist E^F with $d_2(E^F/K) = d_2(E/K) + 2$.*

Proof. This is proved here for curves that do not have a cyclic 4-isogeny defined over $K(E[2])$ and proved for curves that acquire a cyclic 4-isogeny over $K(E[2])$ in Appendix A. The proof in the appendix works for both types of curves, but the proof presented here for curves that do not have a cyclic 4-isogeny defined over $K(E[2])$ is far less complex.

Suppose that E does not have a cyclic 4-isogeny defined over M . By Lemma 4.1, M and M' are disjoint quadratic extensions of K . We may therefore find $\sigma \in G_K$ such that $\sigma|_M \neq 1$ and $\sigma|_{M'} = 1$. Let N be a finite Galois extension of K containing MM' and the ray class field $K(8\Delta_E\infty)$ such that the restriction of $\text{Sel}_2(E/K)$ to N is trivial. Let \mathfrak{p}_1 and \mathfrak{p}_2 be primes of K away from 2 where E has good reduction such that $\text{Frob}_{\mathfrak{p}_1}$ in $\text{Gal}(N/K)$ is the conjugacy class of $\sigma|_N$ and $\text{Frob}_{\mathfrak{p}_2}$ in $\text{Gal}(N/K)$ is the conjugacy class of $\sigma^{-1}|_N$. Since $\sigma\sigma^{-1}|_{K(8\Delta_E\infty)} = 1$, $\mathfrak{p}_1\mathfrak{p}_2$ has a totally positive generator $\pi \equiv 1 \pmod{8\Delta_E}$. Letting $F = K(\sqrt{\pi})$, we get that all places dividing $2\Delta_E\infty$ split in F/K , and that \mathfrak{p}_1 and \mathfrak{p}_2 are the only primes that ramify in F/K .

Since $\gamma|_M \neq 1$, we get that $E(K_{\mathfrak{p}_i}) \simeq \mathbb{Z}/2\mathbb{Z}$ and therefore that $H_f^1(K_{\mathfrak{p}_i}, E[2]) \simeq E[2]/C$, where the isomorphism is given by evaluation at $\text{Frob}_{\mathfrak{p}_i}$. Applying Proposition 2.8 with $T = \{\mathfrak{p}_1, \mathfrak{p}_2\}$, we get that the localization map $\text{loc}_T : \text{Sel}_2(E/K) \rightarrow H_f^1(K_{\mathfrak{p}_1}, E[2]) \oplus H_f^1(K_{\mathfrak{p}_2}, E[2]) = E[2]/C \times E[2]/C$ is given by $c \mapsto (c(\gamma), c(\gamma^{-1}))$. If $c \in H^1(K, E[2])$, then we have $0 = c(1) = c(\gamma\gamma^{-1}) = c(\gamma) + c(\gamma^{-1})$, giving that $c(\gamma) = -c(\gamma^{-1})$. Letting V_T be the image $\text{Sel}_2(E/K)$ under the localization map, we

therefore get that V_T is contained in the one-dimensional diagonal subspace of $E[2] \times E[2]$. By Proposition 2.8, we then get $d_2(E^F/K) = d_2(E/K)$ or $d_2(E^F/K) = d_2(E/K) + 2$.

Since all places dividing $2\Delta_E\infty$ split in F/K , Proposition 3.8 gives that $H_\phi^1(K_v, C^F) = H_\phi^1(K_v, C)$ for v different from \mathfrak{p}_1 and \mathfrak{p}_2 . Since $\gamma|_{M'} = 1$, we get that $E'(K_{\mathfrak{p}_i}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. As $E(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, Lemma 3.10 shows that $\dim_{\mathbb{F}_2} H_\phi^1(K_{\mathfrak{p}_i}, C^F) = 2$. Plugging this into the product formula for the Tamagawa ratio in Theorem 3.5 gives $\mathcal{T}(E^F/E^{F'}) = 4\mathcal{T}(E/E')$.

We now iteratively apply this process until we obtain a twist such that either $d_2(E^F/K) = d_2(E/K) + 2$ or $\text{ord}_2 \mathcal{T}(E^F/E^{F'}) \geq d_2(E/K) + 2$. If $\text{ord}_2 \mathcal{T}(E^F/E^{F'}) \geq d_2(E/K) + 2$, then this would imply that $d_2(E^F/K) = d_2(E/K) + 2$ as $d_2(E^F/K) \geq \text{ord}_2 \mathcal{T}(E^F/E^{F'})$.

The case where E acquires a cyclic 4-isogeny over $K(E[2])$ is dealt with in Lemma A.4 and Corollary A.5. \square

If E does not have a cyclic 4-isogeny defined over M , then by Lemma 4.1, $E'(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and E' does not have a cyclic 4-isogeny defined over M' . Therefore, by swapping the roles of E and E' and iterating the process in the above proof of Theorem 7.1, we are able to find a twist E^F of E such that $\mathcal{T}(E^F/E'^F) \leq 1$ and $d_2(E^F/K) \simeq d_2(E/K) \pmod{2}$. This observation allows us to prove Theorem 1.1.

Proof of Theorem 1.1. By the above observation, we may replace E with a twist such that $\mathcal{T}(E/E') \leq 1$. Iteratively applying Proposition 6.3 to E , we get a twist of E with 2-Selmer rank r for every $0 \leq r < d_2(E/K)$ with $r \equiv d_2(E/K) \pmod{2}$. Iteratively applying Lemma 7.1 to E , we get a twist of E with 2-Selmer rank r for every $r > d_2(E/K)$ with $r \equiv d_2(E/K) \pmod{2}$. Theorem 1.2 then gives the result.

Further, if E does not have constant 2-Selmer parity, then we obtain the result by first replacing E with a twist E^F such that $d_2(E^F/K) \not\equiv d_2(E/K) \pmod{2}$ and proceeding with exactly the same argument. \square

8. CURVES WHICH ACQUIRE A CYCLIC 4-ISOGENY OVER $K(E[2])$.

For the following section we will let r_1 be the number of real places of K and r_2 be the number of complex places of K .

8.1. Local conditions for curves which acquire a cyclic 4-isogeny over $K(E[2])$. Because of Corollary 4.2, the local conditions for the ϕ -Selmer group of a curve that does not have a cyclic 4-isogeny defined over K but acquires one over $K(E[2])$ satisfy much stronger conditions than those curves without a cyclic 4-isogeny defined over $K(E[2])$. Some of these restrictions have been

previously been shown in [Kla11] and we simply note those here. Because of the technical nature of these results, we leave much of the work to Appendix B.

For this section, we will assume that E is a curve with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not have a cyclic 4-isogeny defined over K but acquires one over $K(E[2])$.

Lemma 8.1. *If E has additive reduction and a place $v \nmid 2$, then $H_\phi^1(K_v, C)$ and $H_\phi^1(K_v, C')$ both have \mathbb{F}_2 -dimension 1.*

Proof. This is Lemma 3.3 in [Kla11]. □

Lemma 8.2. *If $u \in K_v$ with $(u)_v < 0$ and $F = K_v(\sqrt{u})$, then exactly one of $H_\phi^1(K_v, C)$ and $H_\phi^1(K_v, C^F)$ is equal to $K_v^\times / (K_v^\times)^2$.*

Proof. If E is given by a model $y^2 = x^3 + Ax^2 + Bx$, then E^F is given by a model $y^2 = x^3 + uAx^2 + u^2Bx$. The result then follows from Lemma B.1 □

Lemma 8.3. *If E has split multiplicative reduction v then either $H_\phi^1(K_v, C) = 0$ or $H_\phi^1(K_v, C) = K_v^\times / (K_v^\times)^2$. If $H_\phi^1(K_v, C) = K_v^\times / (K_v^\times)^2$ and F_w/K_v is a quadratic extension, then $H_\phi^1(K_v, C^{F_w}) = NF_w^\times / (K_v^\times)^2$. If $H_\phi^1(K_v, C) = 0$, then $\dim_{\mathbb{F}_2} H_\phi^1(K_v, C^{F_w}) = 1$.*

Proof. The proof appears in Appendix B. □

Lemma 8.4. *If v is a non-complex places of E , then there exists a quadratic (or trivial) extension F_w/K_v such that $H_\phi^1(K_v, C^{F_w}) \neq H^1(K_v, C)$.*

Proof. This is a combination of Lemmas 8.1 8.2, 8.3, and B.4 and Corollaries B.2 and B.3. □

8.2. Proof Theorem 1.3. The proof of Theorem 1.1 required finding a twist E^F of E such that $\mathcal{T}(E^F/E'^F) \leq 1$. As seen in [Kla11], this will not always be possible if E has a cyclic 4-isogeny defined over K . However, we are able to prove the following:

Lemma 8.5. *If E is an elliptic curve defined over K that does not have a cyclic 4-isogeny defined over K but acquires one over $K(E[2])$, then E has a quadratic twist E^F such that $\text{ord}_2 \mathcal{T}(E^F/E'^F) \leq r_2$. Further, if E does not have constant 2-Selmer parity, then E has a quadratic twist $E^{F'}$ such that $\text{ord}_2 \mathcal{T}(E^{F'}/E'^{F'}) \leq r_2 + 1$ and $d_2(E^{F'}/K) \not\equiv d_2(E^F/K) \pmod{2}$.*

Proof. By Lemma 8.4, we can find a quadratic (or trivial) extension F_w of each completion K_v of K such that $H_\phi^1(K_v, C^{F_w}) \neq H^1(K_v, C)$ for all non-complex places $v \mid 2\Delta_E$. We can use an idelic construction to combine this local behavior into a single global extension.

Define an idele \mathbf{x} of K by $\mathbf{x} = (x_v)$, where x_v is an element of K_v such that F_w is given by $F_w = K_v(\sqrt{x_v})$ for each non-complex place v above $2\Delta_E\infty$ and $x_v = 1$ at all other places v of K . Let \mathbf{d} be the formal product of all places v above $\Delta_E\infty$ and let $\gamma = [\mathbf{x}, MK(8\mathbf{d})]$ be the image of \mathbf{x} under the global Artin map. If \mathfrak{p} is taken to be a prime of K away from $2\Delta_E$ such that $\text{Frob}_{\mathfrak{p}}$ in $MK(8\mathbf{d})$ is γ , then \mathfrak{p} is principal with a generator π such that $K_v(\sqrt{\pi}) = F_w$ for every non-complex place $v \mid 2\Delta_E\infty$. Setting $F = K(\sqrt{\pi})$, we therefore have that $\dim_{\mathbb{F}_2} H^1_{\phi}(K_v, C^F) \leq \dim_{\mathbb{F}_2} H^1(K_v, C) - 1$ for all non-complex places $v \mid 2\Delta_E\infty$. Since E has good reduction at all $v \nmid 2\mathfrak{p}\Delta_E\infty$ and additive reduction at \mathfrak{p} , Lemma 8.1 gives that $\dim_{\mathbb{F}_2} H^1_{\phi}(K_v, C^F) \leq \dim_{\mathbb{F}_2} H^1(K_v, C) - 1$ for all non-complex places v of K .

By Theorem 3.5, $\text{ord}_2 \mathcal{T}(E^F/E'^F)$ is given by $\text{ord}_2 \mathcal{T}(E^F/E'^F) = \sum_{v \text{ of } K} \dim_{\mathbb{F}_2} H^1_{\phi}(K_v, C^F) - 1$. We then have that

$$\begin{aligned} \text{ord}_2 \mathcal{T}(E^F/E'^F) &\leq -(r_1 + r_2) + \sum_{v \mid 2} \dim_{\mathbb{F}_2} H^1(K_v, C) - 2 \\ &= -(r_1 + r_2) + \sum_{v \mid 2} [K : \mathbb{Q}_2] = -(r_1 + r_2) + [K : \mathbb{Q}] = r_2, \end{aligned}$$

where the inequality follows from the fact that $H^1(K_v, C) \simeq K_v^{\times}/(K_v^{\times})^2$ and the first equality further following from the fact that $\dim_{\mathbb{F}_2} H^1(K_v, C) = 2 + [K_v : \mathbb{Q}_2]$ for places $v \mid 2$.

By Theorem 3.6, if E does not have constant 2-Selmer parity, there must be some twist E^L of E such that $\text{ord}_2 \mathcal{T}(E/E') \not\equiv \text{ord}_2 \mathcal{T}(E^L/E'^L) \pmod{2}$ and therefore some place v_0 such that $\dim_{\mathbb{F}_2} H^1(K_{v_0}, C) \not\equiv \dim_{\mathbb{F}_2} H^1(K_{v_0}, C^L) \pmod{2}$. By Lemma 8.1, $\dim_{\mathbb{F}_2} H^1(K_v, C^L) = 1$ for all places $v \nmid 2$ where E^L has additive reduction and it therefore follows that $v_0 \mid 2\Delta_E\infty$. Locally, L/K_v is given by $K_v(\sqrt{u})$ where $u \in K_v^{\times} - (K_v^{\times})^2$. Define an idele $\mathbf{y} = (y_v)$ of K by $y_v = x_v$ for $v \neq v_0$ and $y_{v_0} = u$ if $\dim_{\mathbb{F}_2} H^1_{\phi}(K_{v_0}, C^F) \equiv H^1_{\phi}(K_{v_0}, C) \pmod{2}$ and $y_{v_0} = 1$ if $\dim_{\mathbb{F}_2} H^1_{\phi}(K_{v_0}, C^F) \not\equiv H^1_{\phi}(K_{v_0}, C) \pmod{2}$.

Let \mathbf{d} be the formal product of all places v above $\Delta_E\infty$ and let $\gamma' = [\mathbf{y}, MK(8\mathbf{d})]$ be the image of \mathbf{y} under the global Artin map. If we take a prime \mathfrak{p}' of K away from $2\Delta_E$ such that $\text{Frob}_{\mathfrak{p}'}$ in $MK(8\mathbf{d})$ is γ' , then \mathfrak{p}' is principal. Let π' be a generator of \mathfrak{p}' and set $F' = K(\sqrt{\pi'})$. Calculations similar to those above then show that $\text{ord}_2 \mathcal{T}(E^{F'}/E'^{F'}) \leq r_2 + 1$ and that $\text{ord}_2 \mathcal{T}(E^{F'}/E'^{F'}) \not\equiv \text{ord}_2 \mathcal{T}(E^F/E'^F) \pmod{2}$. Theorem 3.6 then shows that $d_2(E^F/K) \not\equiv d_2(E^{F'}/K) \pmod{2}$, completing the result. \square

Remark 8.6. As the result in [Kla11] was shown by exhibiting an infinite family of curves with $\text{ord}_2 \mathcal{T}(E^F/E'^F) \geq r_2$ for every curve E and quadratic extension F/K , Lemma 8.5 is the best such result we can hope for without further conditions on E .

We are now able to prove Theorem 1.3.

Proof of Theorem 1.3. By Lemma 8.5, we may replace E with a twist such that $\text{ord}_2 \mathcal{T}(E^{F_1}/E'^{F_1}) \leq r_2$. Iteratively applying Proposition 6.3 to E^{F_1} , we get a twist of E with 2-Selmer rank r for every $\text{ord}_2 \mathcal{T}(E^{F_1}/E'^{F_1}) \leq r < d_2(E^{F_1}/K)$ with $r \equiv d_2(E^{F_1}/K) \pmod{2}$. Iteratively applying Lemma 7.1 to E^{F_1} , we get a twist of E with 2-Selmer rank r for every $r \geq d_2(E^{F_1}/K)$ with $r \equiv d_2(E^{F_1}/K) \pmod{2}$. If E does not have constant 2-Selmer parity, then we can additionally find a twist E^{F_2} of E such that $\text{ord}_2 \mathcal{T}(E^{F_3}/E'^{F_3}) \leq r_2 + 1$ and $d_2(E^{F_2}/K) \not\equiv d_2(E^{F_1}/K) \pmod{2}$. Iteratively applying Proposition 6.3 to E^{F_2} , we get a twist of E with 2-Selmer rank r for every $\text{ord}_2 \mathcal{T}(E^{F_2}/E'^{F_2}) \leq r < d_2(E^{F_2}/K)$ with $r \equiv d_2(E^{F_1}/K) \pmod{2}$. Iteratively applying Lemma 7.1 to E^{F_2} , we get a twist of E with 2-Selmer rank r for every $r \geq d_2(E^{F_2}/K)$ with $r \equiv d_2(E^{F_2}/K) \pmod{2}$. Theorem 1.2 applied to all of these twists then gives the result. \square

Proof of Theorem 1.4. Parts (i) and (ii) of Theorem 1.4 are largely a consequence of the fact that $\mathcal{T}(E/E') = \mathcal{T}(E'/E)^{-1}$. However, proving part (iii) additionally relies on techniques similar to those used to prove Lemma 8.5.

Since $\mathcal{T}(E/E') = \mathcal{T}(E'/E)^{-1}$, either $\mathcal{T}(E/E') \leq 1$ or $\mathcal{T}(E'/E) \leq 1$. Therefore, by possibly exchanging the roles of E and E' , we may assume that $\mathcal{T}(E/E') \leq 1$. Iteratively applying Proposition 6.3 to E we get a twist of E with 2-Selmer rank r for every $0 \leq r < d_2(E/K)$ with $r \equiv d_2(E/K) \pmod{2}$. Iteratively applying Proposition A.5 to E we get a twist of E with 2-Selmer rank r for every $r > d_2(E/K)$ with $r \equiv d_2(E/K) \pmod{2}$. Part (i) then follows from applying Theorem 1.2.

If E does not have constant 2-Selmer parity, then we can find a twist E^F of E with $d_2(E^F/K) \not\equiv d_2(E/K) \pmod{2}$. Applying part (i) of this theorem to E^F proves (ii).

To show (iii), we use an idelic argument to show that if E has such a place, then E has a twist E^F with $d_2(E^F/K) \not\equiv d_2(E/K) \pmod{2}$ and $\text{ord}_2 \mathcal{T}(E^F/E'^F) = \text{ord}_2 \mathcal{T}(E/E') \pm 1$.

Let v_0 be a place of K such that either v_0 is real or E has multiplicative reduction at v_0 . Pick $u \in (K_{v_0}^\times) - (K_{v_0}^\times)^2$ such that $K_{v_0}(\sqrt{u}) \simeq \mathbb{C}$ if v_0 is a real place and $K_{v_0}(\sqrt{u})$ is unramified if v_0 is non-archimedean. Define an idele $\mathbf{x} = (x_v)$ of K by $x_{v_0} = u$ and $x_v = 1$ for all $v \neq v_0$. Let \mathbf{d} be the formal product of all places v above $\Delta_E \infty$ and let $\gamma = [\mathbf{x}, MK(8\mathbf{d})]$ be the image of \mathbf{x} under the global Artin map. If \mathfrak{p} is taken to be a prime of K away from $2\Delta_E$ such that $\text{Frob}_{\mathfrak{p}}$ in $MK(8\mathbf{d})$ is γ , then \mathfrak{p} is principal with a generator π . Setting $F = K(\sqrt{\pi})$, we then get that all $v \mid 2\Delta_E \infty$ different from v_0 split in F/K and therefore that $H_\phi^1(K_v, C^F) = H_\phi^1(K_v, C)$ for all $v \mid 2\Delta_E \infty$ different from v_0 . By Lemma 8.1, since E^F has additive reduction at \mathfrak{p} , $\dim_{\mathbb{F}_2} H_\phi^1(K_v, C^F) = 1$.

By the product formula in Theorem 3.5, we therefore get that

$$\text{ord}_2 \mathcal{T}(E/E') - \text{ord}_2 \mathcal{T}(E^F/E'^F) = \dim_{\mathbb{F}_2} H_\phi^1(K_{v_0}, C) - \dim_{\mathbb{F}_2} H_\phi^1(K_{v_0}, C^F).$$

If v_0 is a real place, then Lemma 8.2 gives that exactly one of $H_\phi^1(K_{v_0}, C)$ and $H_\phi^1(K_{v_0}, C^F)$ has \mathbb{F}_2 -dimension one and that the other has \mathbb{F}_2 -dimension zero. If v_0 is a place where E has multiplicative reduction, then exactly one of E and E^F has split multiplicative reduction at v_0 and the other has non-split multiplicative reduction at v_0 . Applying Lemma 8.3, we therefore get that $\dim_{\mathbb{F}_2} H_\phi^1(K_{v_0}, C) - \dim_{\mathbb{F}_2} H_\phi^1(K_{v_0}, C^F) = \pm 1$. In either case, we get that $\text{ord}_2 \mathcal{T}(E^F/E'^F) = \text{ord}_2 \mathcal{T}(E/E') \pm 1$. Theorem 3.6 then shows that $d_2(E^F/K) \not\equiv d_2(E/K) \pmod{2}$.

Now, either both $\mathcal{T}(E/E') \leq 1$ and $\mathcal{T}(E^F/E'^F) \leq 1$ or both $\mathcal{T}(E'/E) \leq 1$ and $\mathcal{T}(E'^F/E'^F) \leq 1$. We can therefore insist that the choice of E or E' that gives the even parities in part (ii) be the same as the choice of E or E' that gave the odd parities. \square

Proof of Corollary 1.5. If either $d_2(E/K) \equiv 0 \pmod{2}$ or E does not have constant 2-Selmer parity, then Theorem 1.1 and Theorem 1.4 imply that either $N_0(E/K, X) \gg \frac{X}{(\log X)}$ or $N_0(E'/K, X) \gg \frac{X}{(\log X)}$. As E and E' have the same Mordell-Weil rank, the result follows. \square

Proof of Corollary 1.7. If either $d_2(E/K) \equiv 1 \pmod{2}$ or E does not have constant 2-Selmer parity, then Theorem 1.1 and Theorem 1.4 imply that either $N_1(E/K, X) \gg \frac{X}{(\log X)}$ or $N_1(E'/K, X) \gg \frac{X}{(\log X)}$. Assuming conjecture III $T_2(K)$ holds, then all curves with 2-Selmer rank one have Mordell-Rank one. As E and E' have the same Mordell-Weil rank, the result follows. \square

REFERENCES

- [Cas65] J.W.S. Cassels. Arithmetic on curves of genus 1. VIII: On the conjectures of Birch and Swinnerton-Dyer. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1965(217):180–199, 1965.
- [DD11] T. Dokchitser and V. Dokchitser. Root numbers and parity of ranks of elliptic curves. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 658:39–64, 2011.
- [FG08] EV Flynn and C. Grattoni. Descent via isogeny on elliptic curves with large rational torsion subgroups. *Journal of Symbolic Computation*, 43(4):293–303, 2008.
- [HB94] DR Heath-Brown. The size of Selmer groups for the congruent number problem, II. *Inventiones mathematicae*, 118(1):331–370, 1994.
- [Kan10] D.M. Kane. On the ranks of the 2-Selmer groups of twists of a given elliptic curve. *Preprint available at <http://arxiv.org/abs/1009.1365>*, 2010.
- [Kla11] Zev Klagsbrun. A family of elliptic curves with a lower bound on 2-Selmer ranks of quadratic twists. *Arxiv preprint available at <http://arxiv.org/abs/1201.5407>*, 2011.
- [KMR11] Z. Klagsbrun, B Mazur, and K. Rubin. Selmer ranks of quadratic twists of elliptic curves. *Preprint available at <http://arxiv.org/pdf/1111.2321v1>*, 2011.

- [Kra81] K. Kramer. Arithmetic of elliptic curves upon quadratic extension. *Transactions of the American Mathematical Society*, 264(1):121–135, 1981.
- [Mil06] J.S. Milne. *Arithmetic duality theorems*. Citeseer, 2006.
- [MR07] B. Mazur and K. Rubin. Finding large Selmer rank via an arithmetic theory of local constants. *Annals of Mathematics*, 166:579–612, 2007.
- [MR10] B. Mazur and K. Rubin. Ranks of twists of elliptic curves and Hilbert’s tenth problem. *Inventiones mathematicae*, 181(3):541–575, 2010.
- [OS98] K. Ono and C. Skinner. Non-vanishing of quadratic twists of modular l-functions. *Inventiones mathematicae*, 134(3):651–660, 1998.
- [SD08] P. Swinnerton-Dyer. The effect of twisting on the 2-Selmer group. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 145, pages 513–526. Cambridge Univ Press, 2008.
- [Sil94] JH Silvermann. Advanced topics in the arithmetic of elliptic curves. *Graduate texts in math*, 151, 1994.
- [Sil09] J.H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Verlag, 2009.
- [SSD05] A. Skorobogatov and P. Swinnerton-Dyer. 2-descent on elliptic curves and rational points on certain Kummer surfaces. *Advances in Mathematics*, 198(2):448–483, 2005.

APPENDICES

APPENDIX A. PROOFS OF LEMMAS 6.2 AND 7.1 WHEN E ACQUIRES A CYCLIC 4-ISOGENY OVER $K(E[2])$

A.1. Generalized Selmer Structures. An important part of the proofs of Lemmas 6.2 and 7.1 can be thought of most naturally in terms of Selmer structures. We outline the relevant parts of theory below.

Let K be a number field and A a G_K -module. For each finite place v of K , define the **unramified local cohomology group** $H_u^1(K_v^{\text{ur}}, A) \subset H^1(K_v, A)$ by

$$H_u^1(K_v, A) = \ker \left(H^1(K_v, A) \xrightarrow{\text{res}} H^1(K_v^{\text{ur}}, A) \right),$$

where K_v^{ur} is the maximal unramified extension of K_v .

Definition A.1. A **Selmer structure** \mathcal{F} for A is a collection of local cohomology subgroups $H_{\mathcal{F}}^1(K_v, A) \subset H^1(K_v, A)$ for each place v of K such that $H_{\mathcal{F}}^1(K_v, A)$ is equal to the unramified local subgroup $H_u^1(K_v, A)$ for all but finitely many places v . We define the **Selmer group** associated to the Selmer structure \mathcal{F} , denoted $H_{\mathcal{F}}^1(K, A)$ by

$$H_{\mathcal{F}}^1(K, A) = \ker \left(H^1(K, A) \xrightarrow{\text{res}_v} \bigoplus_{v \text{ of } K} H^1(K_v, A) / H_{\mathcal{F}}^1(K_v, A) \right).$$

Let A be a finitely generated G_K -module ramified at a finite set of primes. Define the Cartier dual A^* of A as $A^* = \text{Hom}(T, \mu_{p^\infty})$. For a place v of K we have a perfect bilinear Tate pairing

$$H^1(K_v, A) \times H^1(K_v, A^*) \rightarrow H^1(K_v, \mu_{p^\infty}) \xrightarrow{\sim} \mathbb{Q}_p / \mathbb{Z}_p$$

arising from the cup-product pairing. If \mathcal{F} is a Selmer structure on A , then we define a dual Selmer structure \mathcal{F}^* on A^* by setting $H_{\mathcal{F}^*}^1(K_v, A^*) = H_{\mathcal{F}}^1(K_v, A)^\perp$ for each place v of K where \perp is taken with respect to the Tate pairing.

If \mathcal{F}_1 and \mathcal{F}_2 are Selmer structures, we say $\mathcal{F}_1 \leq \mathcal{F}_2$ if $H_{\mathcal{F}_1}^1(K_v, A) \subset H_{\mathcal{F}_2}^1(K_v, A)$ for each place v of K .

Theorem A.2 (Theorem 2.3.4 in [MR07]). *Suppose \mathcal{F}_1 and \mathcal{F}_2 are Selmer structures with $\mathcal{F}_1 \leq \mathcal{F}_2$, then*

(i) *The sequences*

$$0 \rightarrow H_{\mathcal{F}_1}^1(K, A) \rightarrow H_{\mathcal{F}_2}^1(K, A) \xrightarrow{\sum \text{res}_v} \bigoplus_v H_{\mathcal{F}_2}^1(K_v, A) / H_{\mathcal{F}_1}^1(K_v, A)$$

and

$$0 \rightarrow H_{\mathcal{F}_2^*}^1(K, A^*) \rightarrow H_{\mathcal{F}_1^*}^1(K, A^*) \xrightarrow{\sum_{res_v}} \bigoplus_v H_{\mathcal{F}_1^*}^1(K_v, A^*) / H_{\mathcal{F}_2^*}^1(K_v, A^*)$$

are exact where the sum is taken over all places v such that $H_{\mathcal{F}_1^*}^1(K_v, A) \neq H_{\mathcal{F}_2^*}^1(K_v, A)$.

(ii) The images of the right hand maps are orthogonal complements with respect to the sum of the local Tate pairings.

Proof. The first part follows immediately from the definition of Selmer structures. The second is part of Poitou-Tate global duality; see Theorem I.4.10 in [Mil06] for example. \square

Both the 2-Selmer and ϕ -Selmer groups arise from Selmer structures. In the case of the 2-Selmer group, since $E[2]^* = E[2]$ under the Weil pairing and $H_f^1(K_v, E[2])$ is self-dual under the local Tate-pairing, we get that the Selmer group associated to the dual Selmer structure for $\text{Sel}_2(E/K)$ is equal to $\text{Sel}_2(E/K)$. Lemma 3.2 in [MR10] referenced in Section 2.2 then an application of Theorem A.2.

A.2. Proof of Lemma 6.2.

Lemma A.3. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over K but acquires one over $K(E[2])$. If both $d_\phi(E/K) > 1$ and $d_{\hat{\phi}}(E'/K) > 1$, then E has a quadratic twist E^F such that*

- (a) $d_\phi(E^F/K) < d_\phi(E/K)$,
- (b) $d_2(E^F/K) = d_2(E/K)$ or $d_2(E^F/K) = d_2(E/K) - 2$, and
- (c) $\mathcal{T}(E^F/E'^F) \leq \mathcal{T}(E/E')$

Proof. Let $M = K(E[2])$. We begin by recalling that $K(E'[2]) = M$ by Lemma 4.1 and that therefore $\dim_{\mathbb{F}_2} E(K_v)[2] = \dim_{\mathbb{F}_2} E'(K_v)[2]$ for all places v of K by Corollary 4.2.

Pick $R \in E(\overline{K})$ with $2R = P$ and define a co-cycle $c_0 : G_K \rightarrow E[2]$ by $c_0(\sigma) = \sigma(R) - R$ for $\sigma \in G_K$. As E does not have a cyclic 4-isogeny defined over K , there exists some $\gamma_1 \in G_K$ such that $c_0(\gamma_1) \notin C$. Observing that

$$\phi(c_0(\sigma)) = \phi(\sigma(R) - R) = \phi(\sigma(R)) - \phi(R) = \sigma(\phi(R)) - \phi(R)$$

for $\sigma \in G_K$ and recalling that $\phi(R) \in E'[2]$, we see that $c_0(\sigma) \in C$ for all $c \in G_M$ and we therefore get that $\gamma_1 \notin G_M$.

Since $d_\phi(E/K) > 1$ and $d_{\hat{\phi}}(E') > 1$, we can find $b \in \text{Sel}_\phi(E/K)$ and $\hat{b} \in \text{Sel}_{\hat{\phi}}(E'/K)$ such that b does not come from C' and that \hat{b} does not come from C .

Take $N_b = \overline{K}^{\text{Ker } b}$ and $N_{\hat{b}} = \overline{K}^{\text{Ker } \hat{b}}$. Since b does not come from C' and \hat{b} does not come from C , N_b and $N_{\hat{b}}$ are (not necessarily distinct) quadratic extensions of K different from M . We can therefore find $\gamma_2 \in G_K$ such that $\gamma_2|_M = 1$, $\gamma_2|_{N_b} \neq 1$, and $\gamma_2|_{N_{\hat{b}}} \neq 1$. Set $\gamma_3 = (\gamma_1\gamma_2)^{-1} \in G_K$ and observe that $\gamma_3|_M \neq 1$.

Let N be a finite Galois extension of K containing $MK(8\Delta_E\infty)$ such that the restrictions of $\text{Sel}_2(E/K)$, $\text{Sel}_\phi(E/K)$, and $\text{Sel}_\phi(E'/K)$ to N are zero. Choose 3 primes $\mathfrak{p}_1, \mathfrak{p}_2$, and \mathfrak{p}_3 not dividing 2 such that E has good reduction at each \mathfrak{p}_i and $\text{Frob}_{\mathfrak{p}_i}|_N = \gamma_i|_N$ for $i = 1, \dots, 3$. Since $\gamma_1\gamma_2\gamma_3|_{K(8\Delta_E\infty)} = 1$, we get that $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ has a totally positive generator π with $\pi \equiv 1 \pmod{8\Delta_E\infty}$. Letting $F = K(\sqrt{\pi})$, we get that all places dividing $2\Delta_E\infty$ split in F/K , and that $\mathfrak{p}_1, \mathfrak{p}_2$, and \mathfrak{p}_3 are the only primes that ramify in F/K .

We now apply Proposition 2.8 with $T = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}$. Since E has good reduction at $\mathfrak{p}_1, \mathfrak{p}_2$, and \mathfrak{p}_3 it then follows that $H_f^1(K_{\mathfrak{p}_1}, E[2]) = E[2]/(\gamma_1 - 1)E[2] = E[2]/C$, $H_f^1(K_{\mathfrak{p}_2}, E[2]) = E[2]/(\gamma_2 - 1)E[2] = E[2]$, and $H_f^1(K_{\mathfrak{p}_3}, E[2]) = E[2]/(\gamma_3 - 1)E[2] = E[2]/C$ and that the localization map $\text{loc}_T : \text{Sel}_2(E/K) \rightarrow H_f^1(K_{\mathfrak{p}_1}, E[2]) \oplus H_f^1(K_{\mathfrak{p}_2}, E[2]) \oplus H_f^1(K_{\mathfrak{p}_3}, E[2])$ is given by $c \mapsto (c(\gamma_1), c(\gamma_2), c(\gamma_3))$.

As $b \in \text{Sel}_\phi(E/K)$, we may view it as an element of $\text{Sel}_2(E/K)$. Viewing b as a co-cycle, we get that $b(\gamma_2) \neq 0$ since $\gamma_2|_{N_b} \neq 1$ and that $b(\gamma_2) \in C$ since $b \in H^1(K, C)$. Let V_T be the image $\text{Sel}_2(E/K)$ under the localization map. By design, $c_0(\gamma_1) \notin C$. As c_0 represents the element of $\text{Sel}_2(E/K)$ coming from P , we therefore get that V_T has dimension at least 2 in the 4 dimensional space $H_f^1(K_{\mathfrak{p}_1}, E[2]) \oplus H_f^1(K_{\mathfrak{p}_2}, E[2]) \oplus H_f^1(K_{\mathfrak{p}_3}, E[2])$. Noting further that if c is a co-cycle representing an element of $H^1(K, E[2])$, then we have

$$0 = c(\gamma_1\gamma_2\gamma_3) = c(\gamma_1) + c(\gamma_2) + c(\gamma_3) + C,$$

we get that $(Q, 0, 0) \notin V_T$, so that V_T has \mathbb{F}_2 dimension at most 3. Proposition 2.8 therefore gives $d_2(E^F/K) = d_2(E/K)$ or $d_2(E^F/K) = d_2(E/K) - 2$.

By Lemma 3.8, $H_\phi^1(K_v, C^F) = H_\phi^1(K_v, C)$ and $H_\phi^1(K_v, C'^F) = H_\phi^1(K_v, C')$ for all v different from \mathfrak{p}_2 . Define strict and relaxed Selmer groups Z_T and Z^T as

$$Z_T = \ker \left(\text{Sel}_\phi(E/K) \xrightarrow{\text{res}_{\mathfrak{p}_2}} H^1(K_{\mathfrak{p}_2}, C) \right)$$

and

$$Z^T = \ker \left(H^1(K, C) \xrightarrow{\sum \text{res}_v} \bigoplus_{v \neq \mathfrak{p}_2} H^1(K_v, C) / H_\phi^1(K_v, C) \right).$$

Observe that $Z_T \subset \text{Sel}_\phi(E/K), \text{Sel}_\phi(E^F/K) \subset Z^T$ and $Z^{T*} \subset \text{Sel}_\phi(E'/K), \text{Sel}_\phi(E'^F/K) \subset Z_T^*$, where Z_T^* and Z^{T*} are the Selmer groups associated to the dual Selmer structures for Z_T and Z^T respectively.

We now apply Theorem A.2 to the Selmer structures defining Z_T and Z^T , getting that

$$0 \rightarrow Z_T \rightarrow Z^T \xrightarrow{\text{res}_{\mathfrak{p}_2}} H^1(K_{\mathfrak{p}_2}, C)$$

and

$$0 \rightarrow Z^{T*} \rightarrow Z_T^* \xrightarrow{\text{res}_{\mathfrak{p}_2}} H^1(K_{\mathfrak{p}_2}, C')$$

are exact and that the images of the right hand sides are exact orthogonal complements with respect to the local Tate pairing. This means that $\dim_{\mathbb{F}_2} Z^T/Z_T + \dim_{\mathbb{F}_2} Z_T^*/Z^{T*} = 2$. As b is non-zero in Z^T/Z_T and \hat{b} is non-zero in Z_T^*/Z^{T*} , we get that $\dim_{\mathbb{F}_2} Z^T/Z_T = \dim_{\mathbb{F}_2} Z_T^*/Z^{T*} = 1$. By Lemma 3.9, $H_\phi^1(K_{\mathfrak{p}_2}, C^F) \cap H_\phi^1(K_{\mathfrak{p}_2}, C) = 0$, so b does not restrict into $H_\phi^1(K_{\mathfrak{p}_2}, C^F)$. Since b generates Z^T/Z_T , this tells us that $Z^T \cap \text{Sel}_\phi(E^F/K) = Z_T$. Further, $\text{Sel}_\phi(E/K) = Z^T$ since b generates Z^T/Z_T . We therefore get that $d_\phi(E^F/K) = d_\phi(E/K) - 1$.

Finally, since $H_\phi^1(K_{\mathfrak{p}_2}, C^F)$ has \mathbb{F}_2 dimension 1 by Lemma 3.9, the product formula in Lemma 3.5 gives us that $\mathcal{T}(E^F/E'^F) = \mathcal{T}(E/E')$. \square

A.3. Proof of Lemma 7.1.

Lemma A.4. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over K . Then E has a twist E^F with $d_\phi(E^F/K) = d_\phi(E/K) + 1$ such that $d_2(E^F/K) = d_2(E/K)$ or $d_2(E^F/K) = d_2(E/K) + 2$ and $\mathcal{T}(E^F/E'^F) = \mathcal{T}(E/E')$.*

Proof. This lemma is proved by finding two quadratic extension F_1/K and F_2/K such that the Selmer structures for $\text{Sel}_\phi(E^{F_1}/K)$ and $\text{Sel}_\phi(E^{F_2}/K)$ differ from each other and from the Selmer structure for $\text{Sel}_\phi(E/K)$ at a single place \mathfrak{p} . We are then able to show that exactly one of the twists E^{F_1} and E^{F_2} of E has the same ϕ -Selmer rank as E and that the other twist has ϕ -Selmer rank one greater than the ϕ -Selmer rank as E .

Letting $M = K(E[2])$ and $M' = K(E'[2])$. As E does not have a cyclic 4-isogeny defined over K , part (i) of Lemma 4.1 gives us $M' \neq K$, and we can therefore find $\gamma \in \text{Gal}(MM'/K)$ such that $\gamma|_M \neq 1$ and $\gamma|_{M'} \neq 1$. Let N be any finite extension of MM' that is Galois over K such that the restrictions of $\text{Sel}_2(E/K)$, $\text{Sel}_\phi(E/K)$, and $\text{Sel}_{\hat{\phi}}(E'/K)$ to N are trivial. Choose $\sigma_1 \in \text{Gal}(NK(8\Delta_{E\infty})/K)$ such that $\sigma_1|_{MM'} = \gamma$. Now choose two primes, \mathfrak{q}_1 and \mathfrak{q}_2 away from $2\Delta_E$ such that $\text{Frob}_{\mathfrak{q}_1}|_{NK(8\Delta_{E\infty})} = \sigma_1$ and $\text{Frob}_{\mathfrak{q}_2}|_{NK(8\Delta_{E\infty})} = (\sigma_1)^{-1}$. As $\text{Frob}_{\mathfrak{q}_1}\text{Frob}_{\mathfrak{q}_2}|_{K(8\Delta_{E\infty})} = 1$, we get that $\mathfrak{q}_1\mathfrak{q}_2$ has a totally positive generator π' with $\pi' \equiv 1 \pmod{8\Delta_E}$. Define $L = K(\sqrt{\pi'})$.

Now take $\sigma_2 \in \text{Gal}(NLK(8\Delta_{E\infty})/K)$ such that $\sigma_2|_{NK(8\Delta_{E\infty})} = 1$ and $\sigma_2|_L \neq 1$. Since \mathfrak{p}_1 and \mathfrak{p}_2 are ramified in L/K and not in $NK(8\Delta_{E\infty})/K$, we have $L \cap NK(8\Delta_{E\infty})/K = K$ and we can

therefore always find such a σ_2 . Let \mathfrak{p} be any prime away from $2\Delta_E \mathfrak{q}_1 \mathfrak{q}_2$ such that the image of $Frob_{\mathfrak{p}}$ in $\text{Gal}(NLK(8\Delta_E \infty)/K)$ is σ_2 . As $Frob_{\mathfrak{p}}$ in $\text{Gal}(K(8\Delta_E \infty)/K)$ is trivial, \mathfrak{p} has a totally positive generator π with $\pi \equiv 1 \pmod{8\Delta_E}$.

Define quadratic extensions F_1/K and F_2/K by $F_1 = K(\sqrt{\pi})$ and $F_2 = K(\sqrt{\pi\pi'})$. Observe that all places above $2\Delta_E \infty$ split in both F_1/K and F_2/K . The only prime ramified in F_1/K is \mathfrak{p} and the only primes ramified in F_2/K are \mathfrak{q}_1 , \mathfrak{q}_2 , and \mathfrak{p} .

We then apply Proposition 2.8 to E^{F_1} and E^{F_2} with $T_1 = \{\mathfrak{p}\}$ and $T_2 = \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{p}\}$ respectively. Since the images of $Frob_{\mathfrak{q}_1}$ and $Frob_{\mathfrak{q}_2}$ in $\text{Gal}(M/K)$ are non-trivial, $E(K_{\mathfrak{p}_1})[2] \simeq \mathbb{Z}/2\mathbb{Z} \simeq E(K_{\mathfrak{p}_2})[2]$. Since $Frob_{\mathfrak{p}}|_M = 1$, $E(K_{\mathfrak{p}})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The localization map $\text{loc}_{T_1} : \text{Sel}_2(E/K) \rightarrow H_f^1(K_{\mathfrak{p}}, E[2])$ is therefore given by $c \mapsto (c(\sigma_2))$ and the localization map $\text{loc}_{T_2} : \text{Sel}_2(E/K) \rightarrow H_f^1(K_{\mathfrak{q}_1}, E[2]) \oplus H_f^1(K_{\mathfrak{q}_2}, E[2]) \oplus H_f^1(K_{\mathfrak{p}}, E[2])$ is therefore given by $c \mapsto (c(\sigma_1), c(\sigma_1^{-1}), c(\sigma_2))$. As $0 = c(1) = c(\sigma_1 \sigma_1^{-1}) = c(\sigma_1) + \sigma_1 c(\sigma_1^{-1})$, it follows that $c(\sigma_1) = c(\sigma_1^{-1})$ in $E[2]/C$.

Since the image of $Frob_{\mathfrak{p}}$ in $\text{Gal}(N/K)$ is trivial, we get that $G_{K_{\mathfrak{p}}} \subset G_N$. Therefore $\text{loc}_{T_1}(\text{Sel}_2(E/K))$ is trivial and $\text{loc}_{T_2}|_{\text{Sel}_2(E/K)}$ is given by $c \mapsto (c(\sigma_1), c(\sigma_1), 0)$.

Pick $R \in E(\overline{K})$ such that $2R = P$ and define a co-cycle $c_0 : G_K \rightarrow E[2]$ by $c_0(\sigma) = \sigma(R) - R$ for $\sigma \in G_K$. Observing that

$$\phi(c_0(\sigma)) = \phi(\sigma(R) - R) = \phi(\sigma(R)) - \phi(R) = \sigma(\phi(R)) - \phi(R)$$

for $\sigma \in G_K$, we see that $c_0(\sigma) \in C$ if and only if $\phi(R)$ is fixed by σ . As $\phi(R) \in E'[2] - C'$ and $\sigma_1|_{M'} \neq 1$, we therefore see that $c_0(\sigma) \notin C$. As c_0 represents the element of $\text{Sel}_2(E/K)$ coming from C , we therefore get that $\text{loc}_{T_2}(\text{Sel}_2(E/K)) = \langle (Q, Q, 0) \rangle$. By Proposition 2.8, we then get that $d_2(E^{F_i}/K) = d_2(E/K)$ or $d_2(E^{F_i}/K) = d_2(E/K) + 2$ for $i = 1, 2$.

By Lemma 3.8, the local conditions away from \mathfrak{p} for both $\text{Sel}_{\phi}(E^{F_1}/K)$ and $\text{Sel}_{\phi}(E^{F_2}/K)$ are identical to those for $\text{Sel}_{\phi}(E/K)$. Set $T = \{\mathfrak{p}\}$ and define strict and relaxed Selmer groups Z_T and Z^T as

$$Z_T = \ker \left(\text{Sel}_{\phi}(E/K) \xrightarrow{\text{res}_{\mathfrak{p}}} H^1(K_{\mathfrak{p}}, C) \right)$$

and

$$Z^T = \ker \left(\text{Sel}_{\phi}(E/K) \xrightarrow{\text{res}_v} \bigoplus_{v \neq \mathfrak{p}} H^1(K_v, C) / H_{\phi}^1(K_v, C) \right).$$

Observe that $Z_T \subset \text{Sel}_{\phi}(E/K)$, $\text{Sel}_{\phi}(E^F/K) \subset Z^T$ and $Z^{T*} \subset \text{Sel}_{\hat{\phi}}(E'/K)$, $\text{Sel}_{\hat{\phi}}(E'^F/K) \subset Z_T^*$, where Z_T^* and Z^{T*} are the Selmer groups associated to the dual Selmer structures for Z_T and Z^T respectively. Moreover, as the image of $Frob_{\mathfrak{p}}$ in $\text{Gal}(N/K)$ is trivial, we get that $\text{res}_{\mathfrak{p}}(\text{Sel}_{\phi}(E/K))$ is trivial, showing that $\text{Sel}_{\phi}(E/K) = Z_T$. Similarly, $\text{Sel}_{\hat{\phi}}(E'/K) = Z^{T*}$.

Since $\sigma_2|_{MM'} = 1$ we have both $E(K_{\mathfrak{p}})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $E'(K_{\mathfrak{p}})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. As $Frob_{\mathfrak{p}}$ is non-trivial in $L = K(\sqrt{\pi'})$, we get that \mathfrak{p} doesn't split in L and therefore $x^2 - \pi'$ is irreducible mod \mathfrak{p} which means that $\pi' \notin (K_{\mathfrak{p}}^{\times})^2$. Locally, we therefore get that F_1 and F_2 give different ramified extensions of $K_{\mathfrak{p}}$. By Lemma 3.9, we therefore get that $H^1(K_{\mathfrak{p}}, C)$ are $H_{\phi}^1(K_{\mathfrak{p}}, C^{F_1})$, $H_{\phi}^1(K_{\mathfrak{p}}, C^{F_2})$, and $H_u^1(K_{\mathfrak{p}}, C)$ are the three distinct one-dimensional subspaces of $H^1(K_{\mathfrak{p}}, C)$.

We now apply Theorem A.2 to the Selmer structures defining Z_T and Z^T , getting that

$$0 \rightarrow Z_T \rightarrow Z^T \xrightarrow{res_{\mathfrak{p}_2}} H^1(K_{\mathfrak{p}_2}, C)$$

and

$$0 \rightarrow Z^{T*} \rightarrow Z_T^* \xrightarrow{res_{\mathfrak{p}_2}} H^1(K_{\mathfrak{p}}, C)$$

are exact and that the images of the right hand sides are exact orthogonal complements in $H^1(K_{\mathfrak{p}}, C)$. This means that $\dim_{\mathbb{F}_2} Z^T/Z_T + \dim_{\mathbb{F}_2} Z_T^*/Z^{T*} = 2$. As $\text{Sel}_{\phi}(E/K)$ and $\text{Sel}_{\phi}(E'/K)$ restrict trivially into $H^1(K_{\mathfrak{p}}, C)$ and $H^1(K_{\mathfrak{p}}, C')$ respectively and both $\dim_{\mathbb{F}_2} Z^T/\text{Sel}_{\phi}(E/K)$ and $\dim_{\mathbb{F}_2} Z_T^*/\text{Sel}_{\phi}(E'/K)$ are less than or equal to 1, it follows that neither Z^T surjects onto $H^1(K_{\mathfrak{p}}, C)$ nor Z_T^* surjects onto $H^1(K_{\mathfrak{p}}, C')$. This means that both Z^T/Z_T and Z_T^*/Z^{T*} have \mathbb{F}_2 dimension 1 and therefore $res_{\mathfrak{p}}(Z^T)$ is a dimension 1 subspace of $H^1(K_{\mathfrak{p}}, C)$.

Since $Z_T = \text{Sel}_{\phi}(E/K)$, $res_{\mathfrak{p}}(Z^T)$ must be either $H_{\phi}^1(K_{\mathfrak{p}}, C^{F_1})$ or $H_{\phi}^1(K_{\mathfrak{p}}, C^{F_2})$. Choosing F from among F_1 and F_2 such that $res_{\mathfrak{p}}(Z^T) = H_{\phi}^1(K_{\mathfrak{p}}, C^F)$, we get that $Z^T = \text{Sel}_{\phi}(E^F/K)$. We therefore get that $d_{\phi}(E^F/K) = d_{\phi}(E/K) + 1$.

Finally, since $H_{\phi}^1(K_{\mathfrak{p}}, C^F)$ has \mathbb{F}_2 dimension 1 by part (ii) of Lemma 3.9, the product formula in Lemma 3.5 gives us that $\mathcal{T}(E^F/E'^F) = \mathcal{T}(E/E')$. \square

Corollary A.5. *Let E be an elliptic curve defined over a number field K with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not possess a cyclic 4-isogeny defined over K . Then E has a twist E^F with $d_2(E^F/K) = d_2(E/K) + 2$.*

Proof. Iteratively apply Lemma A.4 to E until either $d_2(E^F/K) = d_2(E/K) + 2$ or $d_{\phi}(E^F/K) = d_2(E/K) + 3$. Since E does not have a cyclic 4-isogeny defined over K , the map $\text{Sel}_{\phi}(E/K) \rightarrow \text{Sel}_2(E/K)$ is 2-to-1 by Theorem 3.1 and therefore $d_2(E^F/K) \geq d_{\phi}(E^F/K) - 2$. If $d_{\phi}(E^F/K) = d_2(E/K) + 3$, then $d_2(E^F/K) > d_2(E/K)$, and since $d_2(E^F/K) = d_2(E/K)$ or $d_2(E^F/K) = d_2(E/K) + 2$, it must be in fact that $d_2(E^F/K) = d_2(E/K) + 2$. \square

APPENDIX B. LOCAL CONDITIONS FOR CURVES WHICH ACQUIRE A CYCLIC 4-ISOGENY OVER
 $K(E[2])$

For this section, we will assume that E is a curve with $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ that does not have a cyclic 4-isogeny defined over K but acquires one over $K(E[2])$.

Lemma B.1. *If v is a real place of K and E is given by a model $y^2 = x^3 + Ax^2 + Bx$, then $H_\phi^1(K_v, C)$ has \mathbb{F}_2 -dimension 1 if $(A)_v < 0$ and $H_\phi^1(K_v, C) = 0$ if $(A)_v > 0$.*

Proof. The discriminant for this model of E is given by $\Delta_E = 16(A^2 - 4B)B^2$ and the discriminant of the corresponding model for E' is given by $\Delta_{E'} = 256(A^2 - 4B)^2B$. By Corollary 4.2, either both $(B)_v > 0$ and $(A^2 - 4B)_v > 0$ or both $(B)_v < 0$ and $(A^2 - 4B)_v < 0$. As the image of C' in $H_\phi^1(K_v, C)$ is generated by $\Delta_E(K_v^\times)^2$ and the image of C in $H_\phi^1(K_v, C')$ is generated by $\Delta_{E'}(K_v^\times)^2$, the latter case can't occur as it would violate Lemma 3.3. We therefore get that $(B)_v > 0$ and $(A^2 - 4B)_v > 0$.

Suppose $(A)_v < 0$. If $x_0 \in K_v$ with $(x_0)_v < 0$, then each of $(x_0^3)_v, (Ax_0^2)_v$, and $(Bx_0)_v$ are negative and therefore, x_0 can't appear as the x -coordinate of any point on $E(K_v)$. Since C has trivial image in $K_v^\times/(K_v^\times)^2$, we therefore get that $H_\phi^1(K_v, C') = 0$. Lemma 3.3 then gives that $H_\phi^1(K_v, C) = K_v^\times/(K_v^\times)^2$. Now suppose $(A)_v > 0$. The curve E' is given by a model $y^2 = x^3 - 2Ax^2 + (A^2 - 4B)x$. Exchanging the roles of E and E' in the above shows that $H_\phi^1(K_v, C) = 0$ and $H_\phi^1(K_v, C') = K_v^\times/(K_v^\times)^2$. \square

Lemma 8.3. *If E has split multiplicative reduction v then either $H_\phi^1(K_v, C) = 0$ or $H_\phi^1(K_v, C) = K_v^\times/(K_v^\times)^2$. If $H_\phi^1(K_v, C) = K_v^\times/(K_v^\times)^2$ and F_w/K_v is a quadratic extension, then $H_\phi^1(K_v, C^{F_w}) = NF_w^\times/(K_v^\times)^2$. If $H_\phi^1(K_v, C) = 0$, then $\dim_{\mathbb{F}_2} H_\phi^1(K_v, C^{F_w}) = 1$.*

Proof. Lemma 3.4 in [Kla11] states that if E has split multiplicative reduction at v with Kodaira symbol I_n and E' has Kodaira symbol I_{2n} at v , then $H_\phi^1(K_v, C) = K_v^\times/(K_v^\times)^2$ and $H^1(K_v, C^F)$ is given by $H^1(K_v, C^F) = N_{F_w/K_v} F_w^\times/(K_v^\times)^2$ for quadratic extensions F_w/K_v .

Since E and E' have split multiplicative reduction at v , E/K_v and E'/K_v are G_{K_v} isomorphic to Tate curves E_q and $E_{q'}$ respectively. The curve E_q can be two-isogenous to three different curves: $E_{q^2}, E_{\sqrt{q}}$, and $E_{-\sqrt{q}}$. We therefore get that $|q'|_v = |q|_v^2$ or $|q'|_v = |q|_v^{\frac{1}{2}}$. Since the Kodaira symbol of E is I_n , where $n = \text{ord}_v q$, it then follows that if E has Kodaira symbol I_n , then E' has Kodaira symbol I_{2n} or E' has Kodaira symbol $I_{\frac{n}{2}}$.

In the case where E has Kodaira symbol I_n and E' has Kodaira symbol I_{2n} , we get that $H_\phi^1(K_v, C) = K_v^\times/(K_v^\times)^2$ and $H_\phi^1(K_v, C^{F_w}) = NF_w^\times/(K_v^\times)^2$ by Lemma 3.4 in [Kla11]. In the case

where E has Kodaira symbol I_n and E' has Kodaira symbol $I_{\frac{n}{2}}$ we get that $H_{\hat{\phi}}^1(K_v, C') = K_v^\times / (K_v^\times)^2$ and $H_{\hat{\phi}}^1(K_v, C'^{F_w}) = NF_w^\times / (K_v^\times)^2$ by applying Lemma 3.4 in [Kla11] with the roles of E and E' exchanged. Applying Lemma 3.3 completes the result. \square

Corollary B.2. *If E has non-split multiplicative reduction at a place v , then $H_{\hat{\phi}}^1(K_v, C) \neq H^1(K_v, C)$.*

Proof. Since E has non-split multiplicative reduction at v , there is some quadratic extension F_w/K_v such that E^{F_w} has split multiplicative reduction at v . As E is the twist of E^{F_w} by F_w/K_v , applying Lemma 8.3 to E^{F_w} gives that either $H_{\hat{\phi}}^1(K_v, C) = NF_w^\times / (K_v^\times)^2$ or that $\dim_{\mathbb{F}_2} H_{\hat{\phi}}^1(K_v, C) = 1$, dependent on whether $H_{\hat{\phi}}^1(K_v, C^{F_w}) = K_v^\times / (K_v^\times)^2$ or $H_{\hat{\phi}}^1(K_v, C^{F_w}) = 0$. \square

Corollary B.3. *If E has split multiplicative reduction at a place v and $F = K_v(\sqrt{u})$ where $u \in O_{K_v}^\times - (O_{K_v}^\times)^2$, then $H_{\hat{\phi}}^1(K_v, C^F) \neq K_v^\times / (K_v^\times)^2$.*

Proof. The curve E^F has non-split multiplicative reduction at v and the result then follows from Corollary B.2 \square

Lemma B.4. *If v is a place above 2, then there exists a quadratic extension F/K_v such that $H_{\hat{\phi}}^1(K_v, C^F) \neq K_v^\times / (K_v^\times)^2$.*

Proof. We begin by showing that if v is a place above 2, then there exists a quadratic extension F/K_v such that $E'^F(K_v)$ has no points of order 4.

Pick a model $y^2 = x^3 + Ax^2 + Bx$ for E . The y -coordinates of the points of order 4 on $E'(\overline{K_v})$ are given by $y_1, y_2, \dots, y_6, -y_1, \dots, -y_6$ for some $y_1, \dots, y_6 \in \overline{K_v}$. Since $v \mid 2$, there are at least 7 non-trivial quadratic extensions of K_v and it therefore follows that there is some quadratic F/K_v such that F is not generated over K_v by any of the y_i . We then get that $E'(F)^{\sigma=-1}$ contains no points of order 4, where σ generates $\text{Gal}(F/K_v)$. As $E'^F(K_v) \simeq E'(F)^{\sigma=-1}$, we get that $E'^F(K_v)$ has no points of order 4.

If $E^F(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, then $\Delta_{E'}$ has a non-trivial image in $H^1(K, C)$, since $\dim_{\mathbb{F}_2} E^F(K_v)[2] \simeq \dim_{\mathbb{F}_2} E'^F(K_v)[2]$ and therefore $H_{\hat{\phi}}^1(K_v, C'^F) \neq 0$. Suppose $E^F(K_v)[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let $Q \in E^F(K_v)[2] - C^F$. The image of Q in $H^1(K, C)$ is trivial if and only if $Q = \hat{\phi}(R)$ for some $R \in E'^F(K_v)$. However, since $Q \in E^F(K_v)[2] - C^F$, R would need to have order 4. As $E'^F(K_v)$ contains no points of order 4, the image of Q is non-trivial in $H^1(K, C)$ and therefore $H_{\hat{\phi}}^1(K_v, C'^F) \neq 0$. Applying Lemma 3.3, we get that $H_{\hat{\phi}}^1(K_v, C^F) \neq K_v^\times / (K_v^\times)^2$. \square